

Hitachi Ops Center Analyzer Detail View

User Guide

This document describes how to use Ops Center Analyzer detail view.

© 2025 Hitachi Vantara, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., Hitachi Vantara, Ltd., or Hitachi Vantara Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AlX, DB2, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

Preface.....	8
Product version.....	8
Release notes.....	8
Accessing product documentation.....	8
Conventions for storage capacity values.....	8
Getting help.....	9
Comments.....	9
Chapter 1: Understanding Analyzer detail view	11
Using Analyzer detail view Health Check.....	11
Understanding the Health Check view.....	13
Identifying the affected resources and metrics.....	15
On-demand real time monitoring for Hitachi Enterprise Storage system.....	17
Managing Health Check Settings.....	20
Downloading Health Check report.....	21
Scheduling Health Check report.....	22
Analyzer detail view resource tree.....	22
Understanding the resource tree view.....	24
Analyzer detail view Global search.....	26
Analyzer detail view Inventory reports.....	30
Accessing the Inventory report.....	30
Scheduling the Analyzer detail view Inventory report.....	31
Analyzer detail view Workload Analysis.....	31
Scheduling the Workload Analysis report.....	32
Analyzer detail view Dashboard view.....	33
Analyzer detail view Alerts view.....	34
Analyzer detail view Reports view (Performance and Configuration).....	36
Analyzer detail view Report Builder.....	38
Analyzer detail view Report Scheduler.....	39
Report schedule workflow.....	39
Scheduling the report.....	40
Viewing and managing report schedule.....	42
Downloading scheduled reports.....	44
Changing report retention.....	45

Chapter 2: Getting started.....	47
Accessing the Analyzer detail view.....	47
Adding detail view users.....	47
Configuring the SMTP server for the Analyzer detail view for detail view	50
Configuring the Syslog server for detail view	52
Editing the Syslog server settings.....	52
Configuring an SNMP Manager.....	53
Using the Advanced Activity Monitor.....	54
Configuring an SMTP server for AAM alerts on the Analyzer probe server.....	55
Configuring an SMTP server for AAM alerts on the Analyzer detail view server.....	56
Using System Diagnostics.....	57
Viewing System Diagnostics.....	58
Chapter 3: Configuring the Analyzer detail view dashboard.....	59
Understanding detail view indicators.....	59
Adding detail view dashboard indicators.....	60
Exporting, importing, and resetting detail view dashboard indicator thresholds.....	61
Editing and deleting detail view dashboard indicators.....	62
Customizing detail view dashboard indicator thresholds.....	63
Chapter 4: Setting up Analyzer detail view alerts.....	65
Adding detail view alerts.....	65
Understanding dynamic thresholds.....	72
Identifying the collection interval.....	73
Identifying the metric value.....	77
Managing detail view alert definitions.....	78
Editing detail view alerts.....	79
Viewing detail view alert summaries.....	84
Viewing detail view alert violations.....	85
Chapter 5: Working with Analyzer detail view reports.....	86
Adding user-defined reports in the resource tree.....	86
Working with the Reports dock.....	87
Adding new reports in the detail view Reports dock.....	87
Adding existing reports from the detail view Reports dock.....	87
Searching detail view report templates.....	88
Exporting detail view reports in batch.....	88
Chapter 6: Using Analyzer detail view reports.....	90
Managing Analyzer detail view report settings.....	90

Changing report scheduling (detail view global options in reports pane).....	91
Using On Zoom (detail view global options).....	92
Changing the detail view report duration.....	92
Changing the detail view report date.....	94
Comparing detail view report intervals.....	94
Changing the view of a report.....	95
Isolating resources in a chart report.....	95
Isolating metrics on a chart report.....	96
Changing the plot method of a chart report.....	96
Changing the threshold of a chart report.....	97
Changing the unit of measure for chart reports.....	97
Viewing the query for an existing report.....	98
Downloading and printing detail view reports.....	99
Adding detail view reports to Favorites.....	99
Understanding the owner name used by the Analyzer detail view	99
Renaming instance-level nodes in the resource tree.....	101
Creating custom reports using the Analyzer detail view Report Builder.....	102
Creating a report using Query Builder.....	102
Creating a Analyzer detail view report using MQL.....	106
Viewing reports in Report Builder.....	107
Viewing a performace report.....	107
Pinning a resource in chart report.....	109
Viewing a configuration report.....	110
Exporting reports.....	111
Using a saved query.....	111
Viewing or editing a query.....	112
Cloning a query.....	112
Deleting a query.....	112
Chapter 7: Administering Analyzer detail view.....	113
Resetting a forgotten Analyzer detail view password.....	113
Checking the Analyzer detail view status.....	113
Monitoring Analyzer detail view alerts.....	113
Changing thresholds for detail view system alerts.....	114
Viewing the system status (operating system).....	114
Viewing for detail view data processing status.....	115
Viewing the status of detail view add-on applications.....	117
Downloading Analyzer detail view diagnostic data.....	117
System notifications.....	118
Managing Analyzer detail view user accounts.....	118
Editing a user.....	119
Deleting a user.....	119

Changing a password.....	120
Resetting a password.....	120
Restricting UI access to Active Directory users	121
Active Directory settings.....	121
Configuring the SSL port.....	122
Verifying the Active Directory domain name.....	124
Matching non-default Active Directory server settings.....	124
Setting an explicit domain name for Active Directory.....	125
Managing Active Directory groups.....	127
Editing the Active Directory group domain name.....	128
Disabling validation for Active Directory sAMAccountName and domain.....	128
Changing the built-in FTP (meghadata) user password.....	130
Managing detail view email groups.....	130
Creating email groups in detail view	130
Editing and deleting email groups in detail view	130
Adding a disclaimer or banner message to the Analyzer detail view login window.....	131
Changing the Analyzer detail view locale	131
Setting the Analyzer detail view time zone.....	131
Managing the Analyzer detail view database size.....	132
Controlling the size of the performance database.....	132
Controlling the size of the backup directory.....	134
Controlling the size of the meghadata directory.....	134
Viewing and updating the Analyzer detail view license.....	135
Resolving the SMTP connection for detail view	135
Using the detail view authentication token.....	136
Viewing the Analyzer detail view schema.....	136
Contents of the MIB file on the Analyzer detail view.....	137
Configuring an SSL certificate (Analyzer detail view server).....	139
Configuring a CA signed SSL certificate (Analyzer detail view server).....	139
Creating a private key and a certificate signing request.....	139
Applying server certificates.....	140
Configuring a self-signed SSL certificate (Analyzer detail view server).....	143
Exporting a self-signed certificate for the Analyzer detail view server.....	146
Checking the expiration dates of certificates for Analyzer detail view server.....	147
Changing the SSL or HTTPS port number of the Analyzer detail view server.....	147
Changing the port for On-demand real time monitoring of Hitachi Enterprise Storage.....	148
Enabling TLS certificate verification for the On-demand real time monitoring.	150

Importing TLS or SSL certificate for the SMTP Server.....	152
Stopping the Analyzer detail view server or Analyzer probe server services..	153
Starting the Analyzer detail view server or Analyzer probe server services....	154
Chapter 8: Troubleshooting.....	156
SSD Endurance report does not show any data.....	156
Storage system models.....	156
Endurance value and drive type.....	156
Real-time data import status is red on the Analyzer detail view UI.....	157
Troubleshooting the Analyzer detail view server or Analyzer probe server.....	158
Connecting to the HDEBBUG shell.....	158
Downloading the debug data file.....	159
Diagnosing a probe using the HDEBBUG shell.....	159
Diagnosing a problem when adding a probe.....	160
Diagnosing a problem after adding a probe.....	160
Editing Analyzer detail view AAM alerts.....	161
Enabling the Advanced Activity Monitor.....	162
Disabling the Advanced Activity Monitor.....	162
Disabling statistics collection for Analyzer detail view System	
Diagnostics.....	163
Enabling statistics collection for Analyzer detail view System Diagnostics	163

Preface

This document describes how to use Ops Center Analyzer detail view.

Product version

This document revision applies to Ops Center Analyzer detail view version 11.0.4-00 or later.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on the Hitachi Vantara documentation website: <https://docs.hitachivantara.com>.

Accessing product documentation

Product user documentation is available on: <https://docs.hitachivantara.com>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1,000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1,000^3$ bytes
1 terabyte (TB)	1,000 GB or $1,000^4$ bytes
1 petabyte (PB)	1,000 TB or $1,000^5$ bytes

Physical capacity unit	Value
1 exabyte (EB)	1,000 PB or 1,000 ⁶ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2 ¹⁰) bytes
1 MB	1,024 KB or 1,024 ² bytes
1 GB	1,024 MB or 1,024 ³ bytes
1 TB	1,024 GB or 1,024 ⁴ bytes
1 PB	1,024 TB or 1,024 ⁵ bytes
1 EB	1,024 PB or 1,024 ⁶ bytes

Getting help

The [Hitachi Vantara Support Website](https://support.hitachivantara.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

[Hitachi Vantara Community](https://community.hitachivantara.com) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.feedback@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Understanding Analyzer detail view

Hitachi Ops Center Analyzer detail view (Analyzer detail view) provides visibility into your storage infrastructure using sophisticated analytics. The product uses various methods to collect metrics, such as IOPS, transfers, and latency, from target devices, and does so without changing data or affecting performance. These metrics are collected by the Analyzer probe server at regular time periods, and then periodically transferred to the Analyzer detail view server for processing. Analyzer detail view builds reports from this processed data using built-in reports and interactive charts. You can use the reports to assess your data center infrastructure to monitor its health and to identify areas of actual and potential problems. Analyzer detail view allows you to monitor your entire infrastructure with the help of a Health Check, dashboard, visual and email alerts, and flexible reporting functions.

Using Analyzer detail view Health Check

Monitoring performance is essential for effective data center management. System administrators require access to resource information at any moment to help understand its performance.

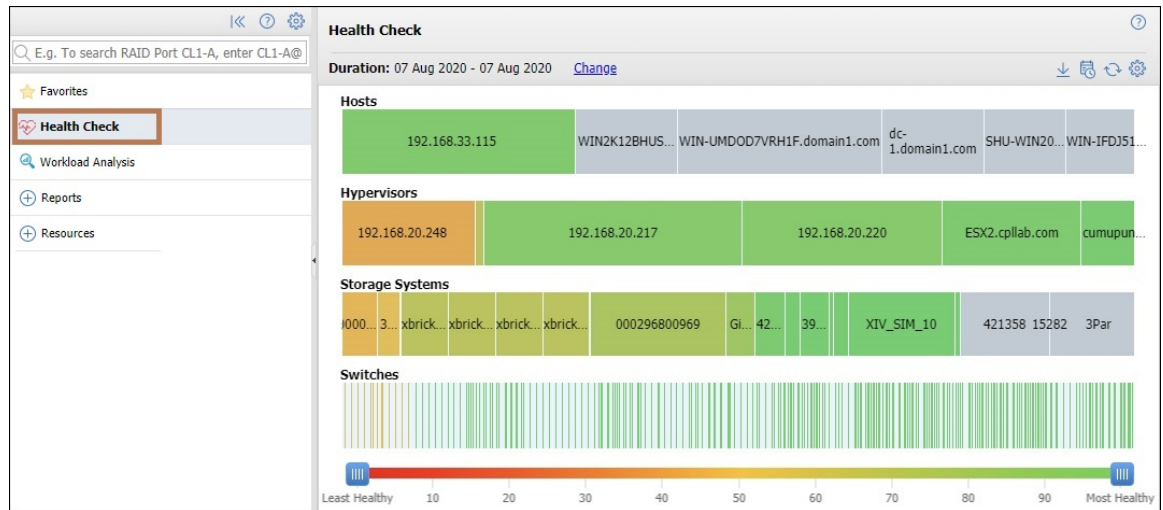
The Analyzer detail view Health Check provides overall visibility of your resources across the monitoring environment (storage systems, switches, hosts, and hypervisors) in treemap view in the same pane, where at a glance the system administrators can identify the problematic area and drill-down to view the health of underlying resources.

The Health Check view indicates overall resource health using the color and size of a block. Where the color represents the health of the resources and the size of the block represents the most relevant attributes of the target, like Capacity for the storage systems, ports for the switches, and so on.

You can download and schedule the Health Check report.



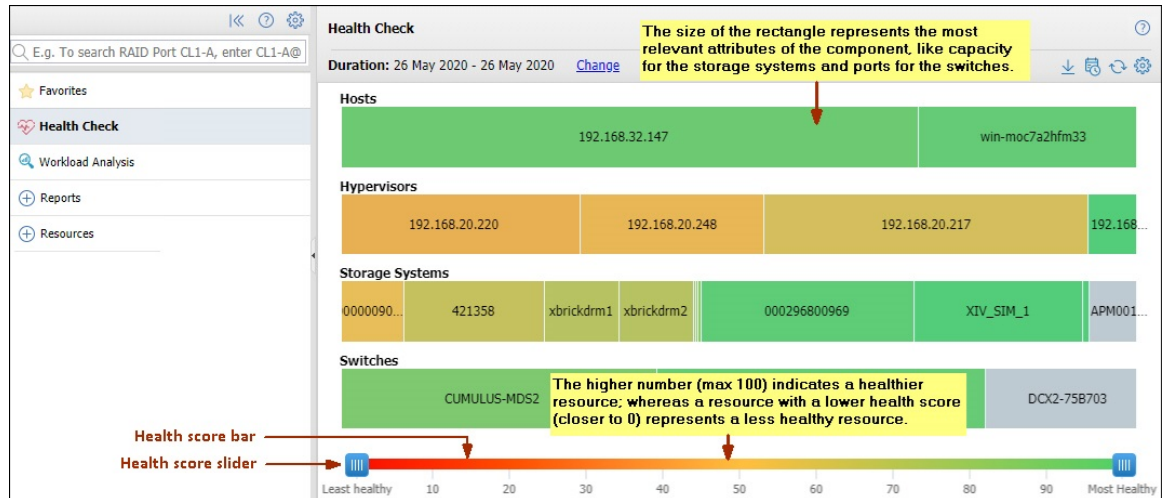
Note: You can navigate to the Health Check view by clicking the Health Check option in the left pane. When you first log on to the Analyzer detail view, Health Check is the default view.



Understanding the Health Check view

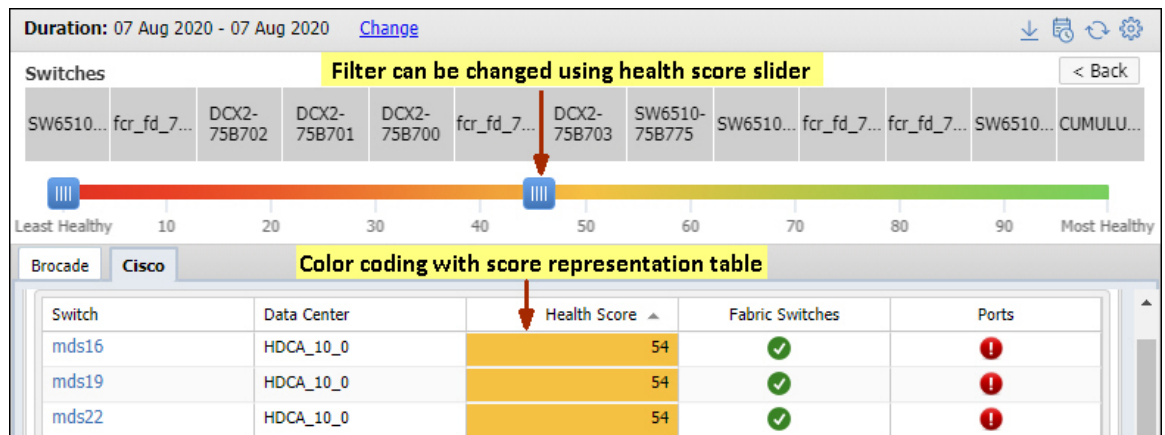
Health Check shows overall resource health using the size of block, health score, and color representation.

- The size of the block represents the most relevant attributes of the target:
 - **Host:** Total Capacity
 - **Hypervisors:** Total Capacity
 - **Storage Systems:** Total Capacity
 - **Switches:** Port count



The grey block in the Health Check view represents that the data is not available or the available data is not sufficient to calculate the health.

- The resource color and score represent its relative health. The health score is a number between 1 and 100 that provides an objective (numerical) view of the health of a resource. The higher number (max 100) indicates a healthier resource; whereas a resource with a lower health score (closer to 0) represents a less healthy resource. The health score is calculated based on the number of times a metric of the resource has exceeded the warning or critical threshold that is defined for that resource and metric combination. A large number of critical and warning thresholds violation leads to a lower score. Similarly, the health is represented in the color, closer to Red means a lower score and closer to Green indicates a higher score.
- You can filter the Health Check view based on the health score with slider (available in health score bar). The slider moves in five unit increments. The filtered state is preserved when you click on any resource and move to next page. The filter can be changed on this page.



Note: Filter on health score does not update the table entries.

- Indicators in the Health Check are also calculated in the similar manner and result is depicted in the traffic light display red (Critical), amber (Warning), and green (Normal) indicators:
 - Green:** Indicates the resource is healthy.
 - Amber:** Indicates the resource is reasonably healthy but the user is cautioned to monitor this resource closely.
 - Red:** Indicates that the resource is not healthy and might require immediate attention.

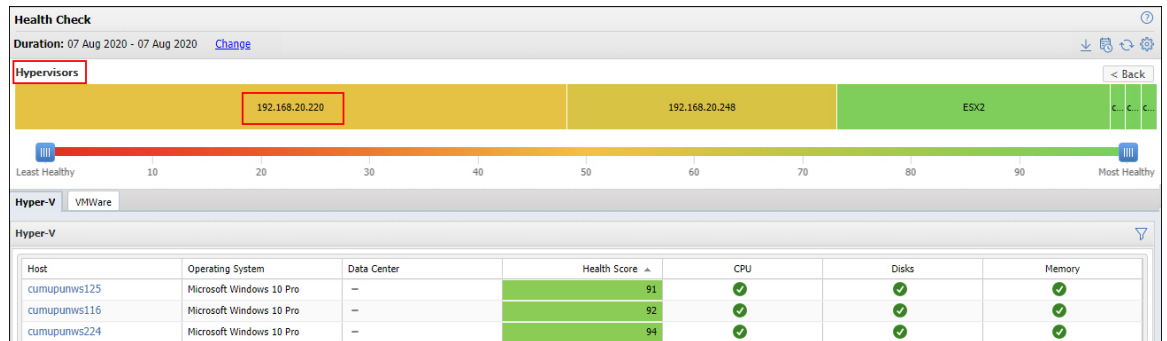
Identifying the affected resources and metrics

You can drill-down in the Health Check view to identify the health of underlying resources.

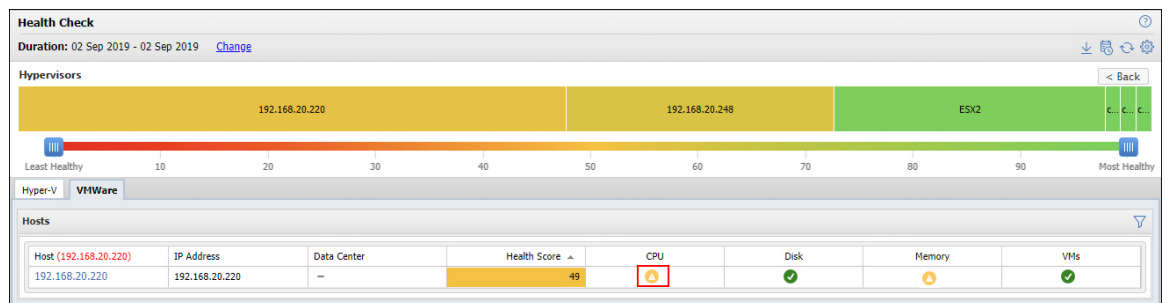
- In the Health Check window, click the most affected resources by identifying its color. In the following example, Hypervisors are indicating a warning. Click the block in the **Hypervisors** section for further details.



- The section specific to the Hypervisors opens, this section shows all the hypervisors targets from your monitoring environment. In Hypervisors, the host 192.168.20.220 is not healthy and requires attention. Click the host block for the details.



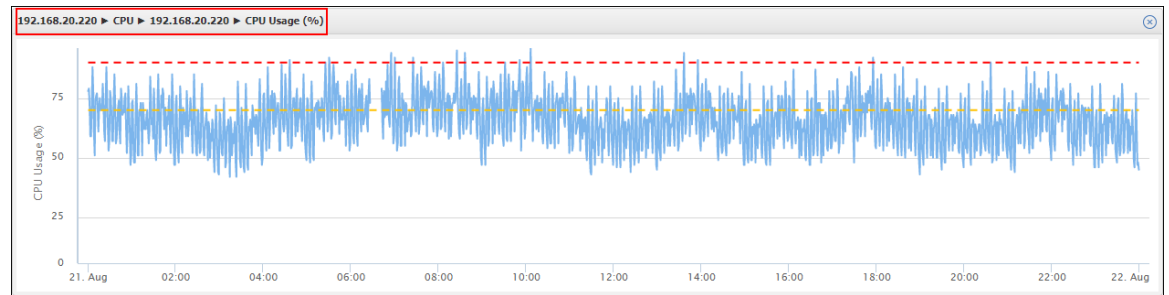
- Because this is a VMware host, the VMware tab opens with details specific to the host 192.168.20.220. In this case, the CPU and Memory indicate that the resource is a possible suspect. For this example let us use CPU to find its detailed health, click the CPU warning icon.



- The details specific to CPU is shown. The health of the CPU is represented with the warning icon. Click the warning icon for further details.

Hyper-V VMware							
Hosts							
Host (192.168.20.220)	IP Address	Data Center	Health Score ▲	CPU	Disk	Memory	VMs
192.168.20.220	192.168.20.220	—	49	▲	✓	▲	✓
192.168.20.220 ► CPU							
Host	IP Address	Operating System	Health Score ▲	CPU Usage (%)			
				Avg	Max	Top 80% Avg	Health
192.168.20.220	192.168.20.220	VMware ESXi	67	65.93	96.00	69.64	▲

In the following example, the performance trends show that the CPU usage is violating the warning and critical thresholds and needs attention.



On-demand real time monitoring for Hitachi Enterprise Storage system

On-demand real time monitoring helps you to view the performance of each RAID LDEV and its related resources (RAID MPB and RAID Port) for every second. When you start the On-demand real time monitoring in the Analyzer detail view Health Check, the Analyzer detail view server connects to RAID Agent server (usually, the host on which the Analyzer probe server is installed) to collect live data and shows it in the reports. This real-time data helps you to perform load balancing of storage system resources.

Currently, On-demand real time monitoring is supported only for the RAID LDEV resource type of Hitachi Enterprise Storage. You can also see a few reports of RAID LDEV related resources (RAID MPB and RAID Port).



Note:

- The real-time data is not saved in the database. However, you can download it as an image (PNG) or CSV data.
- Only one of the users in the Analyzer detail view can view the On-demand real time monitoring at one time.

Before you begin

- Make sure that the Analyzer detail view server can connect to the RAID Agent server using the following::
 - Default port: 24262
 - Default Protocol: WSS

If you want to use other than default port, refer to [Changing the port for On-demand real time monitoring of Hitachi Enterprise Storage \(on page 148\)](#).

- You can use the TLS certificate verification on the Analyzer detail view server to securely connect to the RAID Agent server. By default, it is disabled. To enable it, refer to the [Enabling TLS certificate verification for the On-demand real time monitoring \(on page 150\)](#) section.

Procedure

- In the Health Check window, click the Hitachi Enterprise Storage system block in the **Storage Systems** section.

Health Check

Duration: 25 Aug 2021 - 25 Aug 2021 [Change](#)

Hosts

sanityh1aaaserver.domain1.com	win-moc7a2hfm33	windowshubhangi
-------------------------------	-----------------	-----------------

Hypervisors

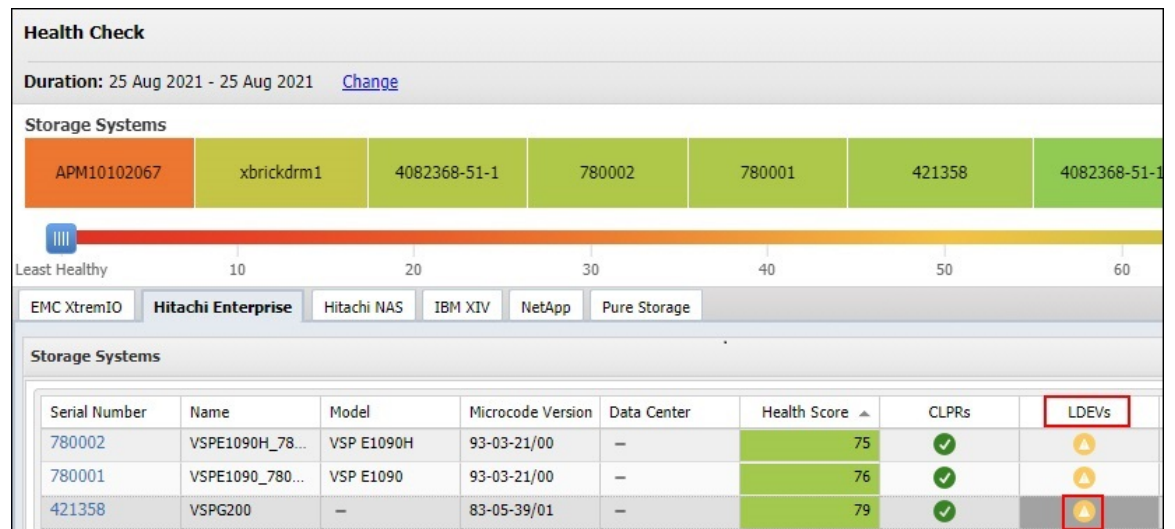
localhost.localdomain	sccmsrv16.domain1.com	
-----------------------	-----------------------	--

Storage Systems

APM10102067	xbrickdrm1	4082368-51-1	780002	780001	421358
-------------	------------	--------------	--------	--------	--------

The storage systems related section opens.

- Click the **Hitachi Enterprise** tab.
The storage systems are listed in a table.
- In the **LDEVs** column, click the health check indicator icon.



All the LDEVs of the storage system are displayed as follows:

Storage Systems

Serial Number	Name	Model	Microcode Version	Data Center	Health Score ▲	CLPRs	LDEVs	MPBs
421358	VSPG200_421358	VSP G200	—	—	79	✓	⚠	✓

421358 ▶ LDEVs Real-time Monitoring

LDEV	Owner	Port	MPB	Health Score ▲	IOPS			Health
					Avg	Max	Top 80% Avg	
00:07:F9	vmware4	CL2-A	MPU-11(1)	9	823.98	1126.00	843.79	⚠
00:00:29	ESX20.246	CL2-A	MPU-20(2)	14	796.84	2746.00	906.28	⚠
00:04:0A	vmware4	CL2-A	MPU-20(2)	45	242.18	661.00	268.97	⚠
00:03:D5	ESX-20.246_2...	CL5-A,CL2-A	MPU-20(2)	54	23.79	419.00	25.04	⚠
00:03:D6	ESX-20.246_2...	CL5-A,CL2-A	MPU-21(3)	61	49.69	307.00	54.50	⚠
00:00:00	—	—	MPU-10(0)	100	0.00	0.00	0.00	✓



Note: You can also navigate to the LDEVs by clicking health check indicator icon in the **Owner** column and then clicking LDEVs number in the **LDEV** column. It helps you to view reports for the LDEVs related to a owner.

- Under the *Storage_system_serial_number* > LDEVs table, select the LDEVs for which you want real-time monitoring.

The **Real-time Monitoring** button is enabled.

- Select the LDEVs for which you want to view the real-time reports.



Note: You can select a maximum of 20 LDEVs.

- Click the **Real-time Monitoring** button.
- Click **Continue** to confirm.

The Analyzer detail view server connects to the RAID Agent server instance for the storage system with the selected RAID LDEV.

A separate browser tab is displayed. It contains a set of pre-defined reports that show the real-time data for the selected LDEVs. It also contains the reports for the related RAID Port and RAID MPB resources.

**Note:**

- The real-time reports display data for a maximum 15 minutes. The reports are refreshed automatically. Do not refresh the window. If you want to restart data collection after 15 minutes, click the **Start Data Collection** button. The data of the previous session is removed and the reports will run for another 15 minutes.
- To stop real-time monitoring, click the **Stop Data Collection** button.
- The real-time data is not preserved after you close the browser tab. To save the data, you can download the reports as an image (PNG) or CSV data using the ≡ button.

Managing Health Check Settings

Health Check has predefined default settings that you can customize to meet your requirements. These settings are user-specific and retained at user level.

Changing the duration

You can change the duration using the **Duration** option. The default duration of the Health Check view is the previous day.

1. To change the duration, click the **Change** link.
2. In the **Duration**, select one of the following options:
 - **Last:** This is a default setting, the Health Check view show the latest available data up to last 1 day. For example, if you are viewing the health on July 28, 2019 (current date), the Last option shows the data until July 27, 2019. You can either choose 1 day or 7 days.
 - **Custom:** You can view a health in custom duration, specify the date range for which you want to view the health (maximum: 7 days).

You can refresh the Health Check view by using the refresh  option.

3. Click **Ok**.

Changing the Health Check view settings

You can change the settings as follows:

- Show or hide the inactive resources
- Number of records to display
- Enable the color cell based on metric value

These settings are available at the upper right corner of the Health Check view and they are applicable to all the types of target.

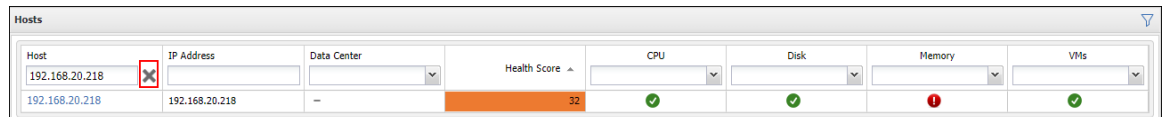
1. At the upper right corner of the Health Check view, click the **Settings**  icon.
2. You can modify the following settings:
 - **Hide inactive resources:** You can choose whether you want to show or hide the inactive resources in tree map. By default, the inactive resources are hidden. A resource is considered inactive when its data is not available or the available data is not sufficient to calculate the health.
 - **Records per page:** You can specify the number of records you want to view per page. (minimum: 10 and maximum: 100)
 - **Color cell based on metric value:** Select the check box to view the records highlighted with a color that represents the value of the metric. Closer to Red means a lower score and closer to Green indicates a higher score.
3. Click **OK** to save the changes.

Applying the filter

You can filter the records based on your requirements.

The Health Check view automatically filters the records of the selected target as you drill-down to view its details. You can remove this filter to view all the records of the target.

1. In the area where target tabs are listed, click the **Toggle Filter**  icon.
 The filter option is shown in each column. In the following example, the Health Check view has automatically applied the filter to records of the selected target as you drill-down.



Host	IP Address	Data Center	Health Score	CPU	Disk	Memory	VMs
192.168.20.218	192.168.20.218	-	32	✓	✓	!	✓

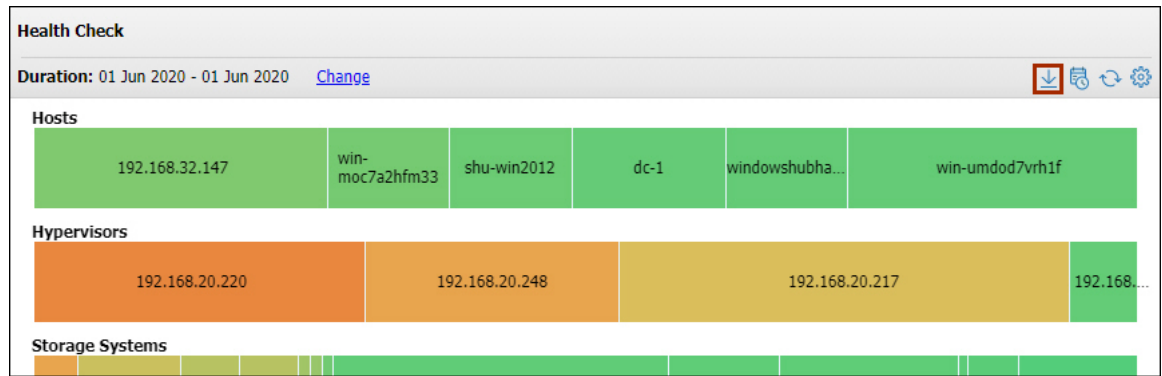
2. To remove the filter, click remove filter  icon.

Downloading Health Check report

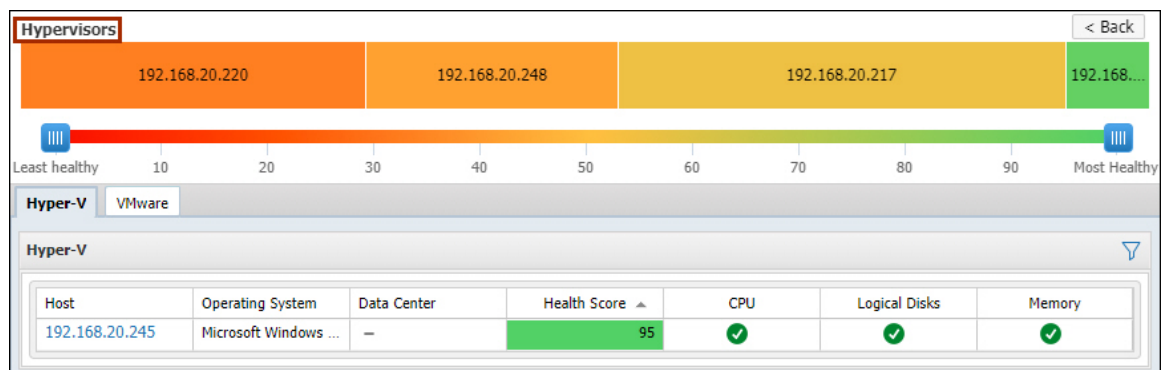
You can download a report in xlsx format for all targets of your monitoring environment or a specific target. The report is based on the active view of the Health Check.

For example,

If you are downloading the report from the topmost view, the report covers all the targets. In the following sample screenshot, the report will be generated for Storage Systems, Switches, Hypervisors, and Hosts.



If you are downloading the report after navigation to a specific target, then the report covers only that specific target. In the following sample screenshot, the report will be generated for the Hyper-V and VMware of the Hypervisors.



- To download a report, click the download  icon at the top right corner of the Health Check view. It might take time to download the report.
 - A Zip file is generated that contains reports for each target type in xlsx format.
 - The Zip contains separate xlsx file for each target type.
 - Each report contains the top 10,000 least healthy records of each target (hosts, hypervisors, storage systems, or switches) and top 10,000 least healthy associated resources (ports, ldevs, and so on).

Scheduling Health Check report

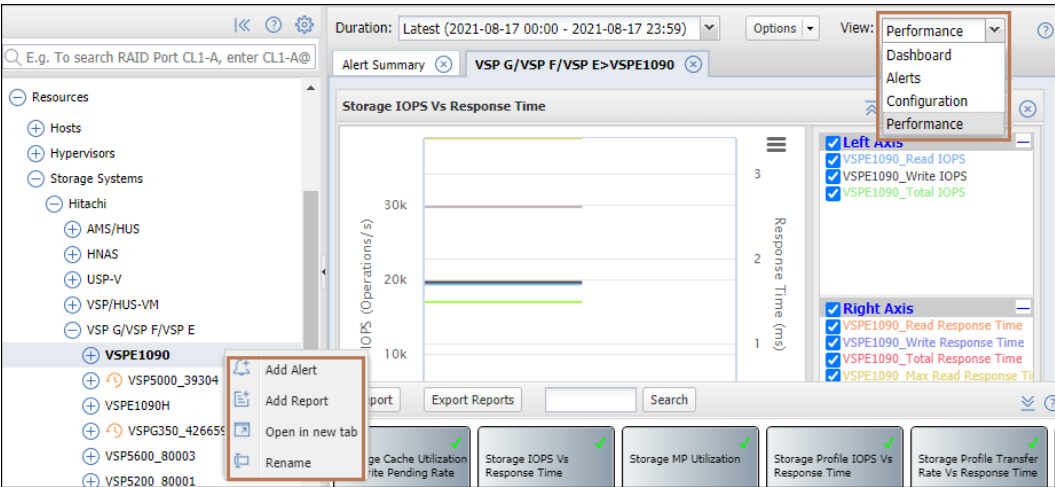
You can schedule Health Check report to receive it over an email by clicking on the  icon at the top right corner of the Health Check window.

For more information, refer to [Report Scheduler \(on page 39\)](#).

Analyzer detail view resource tree

Your entire IT infrastructure is represented in the resource tree (Resources in the left pane). You can navigate the tree, perform searches, rename instance-level nodes, and add alerts or reports.

You can access any resource by navigating through the tree or using the Search field. Clicking a resource opens the currently selected View (in this example, the Dashboard view).

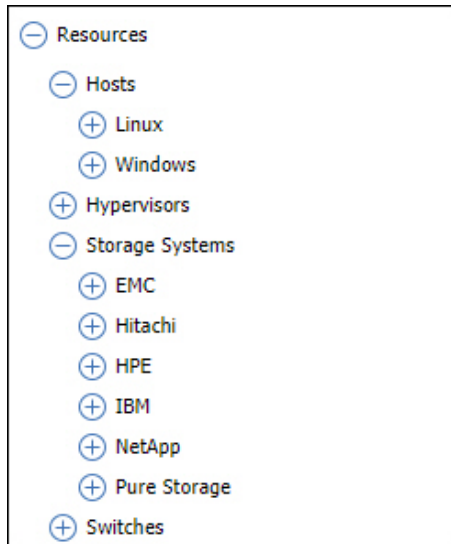


You can also right-click a resource to add a report or alert.

Understanding the resource tree view

The resource tree is the hierarchical representation of the targets and their resources collected by different probes. This section describes various aspects of the resource tree.

- The resource tree contains nodes for Hosts, Hypervisors, Storage Systems, and Switches. Each of these nodes contain subnodes. For example, the Hosts node contains the Linux and Windows subnodes.



- The Storage Systems node includes subnodes related to default and add-on probes. The Hitachi subnode lists the resources collected by the default probes (Hitachi Enterprise Storage and Hitachi NAS). The Hitachi subnode is always displayed even if no license is registered and no data is available in the Analyzer detail view.

Other add-on probe related subnodes such as EMC, HPE, NetApp, and Pure Storage are displayed only when a valid (add-on) license is registered and data is available in the Analyzer detail view.

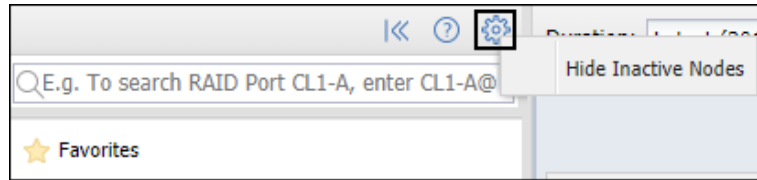
For example, if the data collected by EMC VMAX probe is available on the Analyzer detail view and valid (add-on) license is registered, then only the EMC > VMAX node is displayed and other nodes, such as EMC > XtremIO, HPE, NetApp, and Pure Storage nodes are not displayed in the tree.



Note:

- You can check whether add-on license is registered in the **Manage > Status > License Information**. Click the  icon and then in the **Category** column, select **Third Party Storage**. This is a combined capacity (type) license for EMC VMAX, EMC XtremIO, HPE 3PAR, NetApp, and Pure Storage.
- If the Third Party Storage license has expired on the Analyzer detail view, the add-on probes related subnodes are no longer displayed. However, you can retrieve processed data using MQL (in **Reports > Build** feature) and REST API.
- The Hosts, Hypervisors, and Switches nodes are displayed even if no license is registered and no data is available.
- Nodes are displayed as follows to indicate they are no longer monitored:
 - : The probe has been deleted or the probe is not monitoring the target resource.

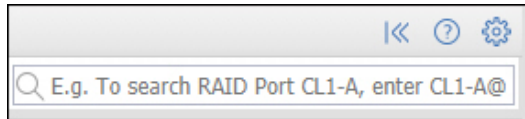
- : The Analyzer detail view has not received data from the probe in the last 30 days. You can hide these nodes by using the Hide Inactive Node option.



- The owner of an Hitachi storage system under the Owners node represents the host or application to which the LDEV is provisioned. If an LDEV is presented to multiple hosts, then the owner name is constructed by combining the host group names.

Analyzer detail view Global search

The Global search helps you to locate and filter a resource in the resource tree. It is available at the top of the left pane.



You can locate and filter the resources using the following methods:

- Type the complete or partial resource name in the Search text box and then press **Enter**. The resource is displayed with its path in resource tree. If a resource is available at different nodes, the path for each node is displayed.

For example:



- If the resources count is large, it is recommended to use the search refinement option as follows:

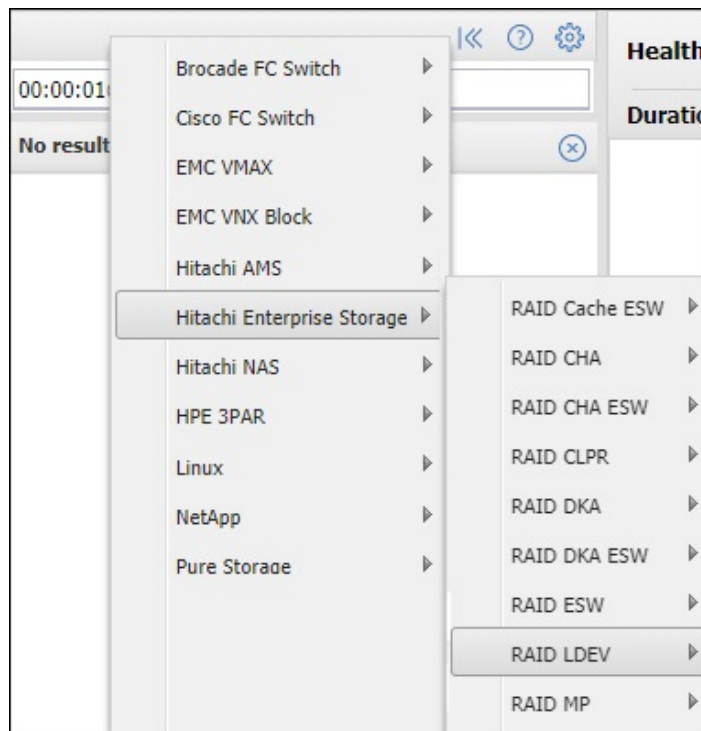
1. Type the @ character in the search text box after the search string.

For example, to search the port CL1-A, type as follows:

CL1-A@

The refinement menu appears.

2. Select the required probe type, resource type, and attribute name (optional).



The resources that match the search are shown as a part of a filtered tree.

3. The search result is shown in the left pane. You can perform the following operations

with the search result:

- Click the search result to expand the node level.
- Click the node or any intervening level to open the corresponding resource reports in the Reports pane.

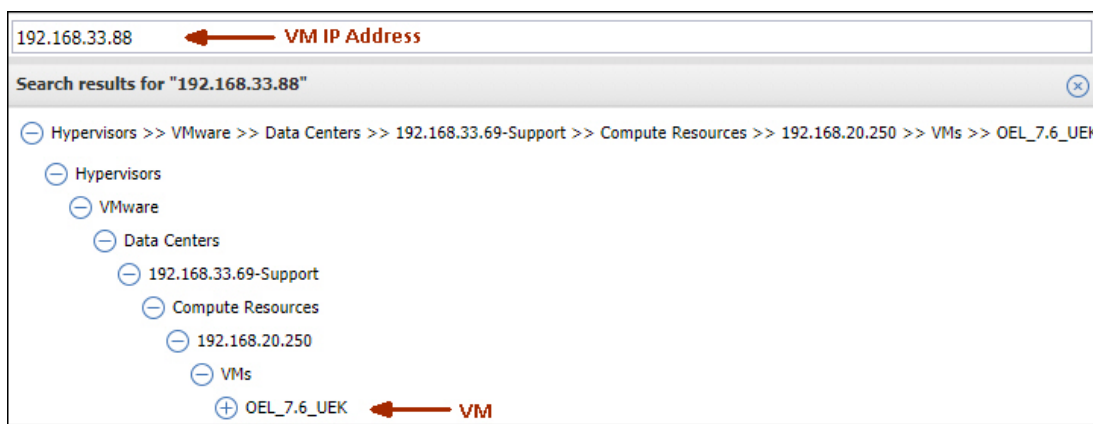


Note: If the search query does not match any result, then the following message appears:

No results matched for `"search-string"`.

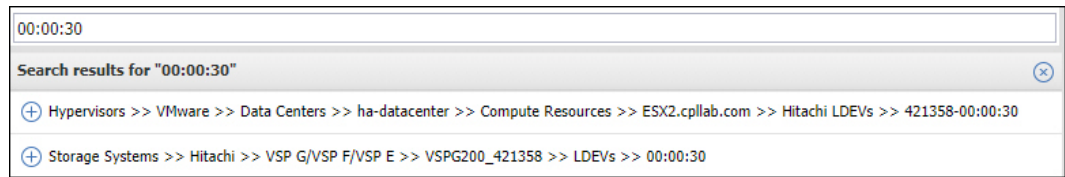
- To exit the search, click the  button. This resets the tree view and search box, but retains the reports in the Reports pane.
- When you search (without search refinement option), the global search feature by default searches the following list of metrics:
 - Name
 - IP Address or IP
 - Serial Number
 - WWN
 - Node WWN
 - FC WWN
 - Port WWN
 - Management IP Address

For example, you can search a VM by its IP address as shown in the following screenshot:



- The search result includes the shortest node path within a target system.
For example, suppose the LDEV 00:00:30 is available under the following nodes in target Hitachi storage systems and VMware vCenter Server:
 - Storage Systems > Hitachi > VSP G/VSP F/VSP E > *Storage-System-Instance* > LDEVs
 - Storage Systems > Hitachi > VSP G/VSP F/VSP E > *Storage-System-Instance* > Parity Groups > Pool Parity Groups > *Pool-Parity-Groups-Instance* > LDEV
 - Hypervisors > VMware > Data Centers > *Data-Center-Instance* > Compute Resources > *Compute-Resources-Instance* > Hitachi LDEVs
 - Hypervisors > VMware > Data Centers > *Data-Center-Instance* > Datastores > *Datastores-Instance* > Disks > *Disks-Instance* > Hitachi LDEVs

In this case, when you search for the LDEV **00:00:30**, the search result will be as follows:



Analyzer detail view Inventory reports

The Analyzer detail view provides a summary of important resources from your storage infrastructure in the Inventory report. You can view a high-level inventory, such as count of components, total capacity, used capacity and its percentage, and so on. You can download and schedule the inventory report.

The Inventory report is available for the following target types:

- Brocade FC Switch
- Cisco FC Switch
- Hitachi Enterprise storage system
- VMware
- Windows or Hyper-V

Accessing the Inventory report

You can view the high-level inventory and download a detailed Inventory report in the Analyzer detail view UI.

Procedure

1. In the left pane, click **Reports > View**.

The report **View** opens with the **Inventory** tab and displays a separate report for each supported target types.

By default, the report shows the latest available data for the last 24 hours. For example, if the data import time is December 23, 2019 10:00 A.M, then the default duration shows the data from December 22, 2019 10:00 A.M to December 23, 2019 09:59 A.M.

2. Specify the duration for the report (maximum: 7 days) and then click **Apply**.

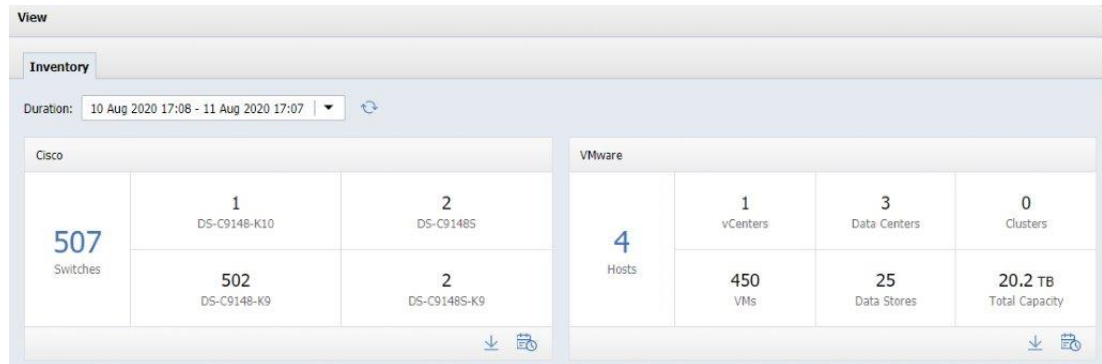
Reports show the high-level inventory on the UI, such as count of components, total capacity, used capacity, and so on. You can also download the detailed Inventory report to view more details in the form of xlsx file.

3. Click  to download the detailed inventory report.

A zip file is generated that contains the report in xlsx format with more detailed information of the target type.

Scheduling the Analyzer detail view Inventory report

You can schedule Inventory reports to get those over an email for offline usage by clicking the  icon at the bottom right corner of each report.



When you click this icon, you are redirected to the **Create** window of the **Report Scheduler**, where you can select the frequency, email alerts and so on. For more information, refer to [Analyzer detail view Report Scheduler \(on page 39\)](#).

Analyzer detail view Workload Analysis

Workload Analysis provides workload information for applications and underlying resources.

For example, based on data in the report, you can identify:

- LDEVs where Adaptive Data Reduction (ADR) should be enabled
- Applications that are affecting storage system performance
- Whether the workload can be migrated to ADR-enabled systems
- Workload of Hitachi Enterprise Storage, VMware infrastructure, Cisco and Brocade switches for key resources and metrics.

You can also determine if your infrastructure needs to be upgraded, such as adding new generation storage systems to handle the workload more efficiently.



Note: Workload Analysis is currently supported for the following:

- Hitachi Enterprise Storage
- VMware
- Brocade FC Switch
- Cisco FC Switch

The screenshot shows the Ops Center Analyzer interface. On the left, the 'Workload Analysis' option is selected in the sidebar. The main area displays a table of storage systems for 'Hitachi Enterprise Storage'. The table has the following data:

Storage System	Serial Number	Max IOPS	Avg IOPS	Max Transfer Rate (MB/s)
VSP5500-30833	30833	-	-	-
VSPE1090H_700031	700031	0.0	0.0	0.0
VSPE1090_700032	700032	0.0	0.0	0.0

Below the table, there are tabs for 'Storage System' and 'Owners'. A 'Download Workload Analysis Report' button is located at the bottom right of the interface.

When you click **Workload Analysis** in the left pane, the devices (such as, storage systems for Hitachi Enterprise Storage) are listed in a table in the right pane. You can change the device types from the **Device Type** list to view the respective devices. The most relevant metrics and their data points are displayed in the table. For Hitachi Enterprise Storage, when you click the data points in the **Max IOPS** column, a report is displayed on the screen to show more data points for additional metrics, such as transfer rate, block size, cache hit rate, and so on. This report contains data points for the Max IOPS value plotted in the table.

When you click a resource, the related chart reports are displayed in tabs below the table. For example, in the screenshot, the **Storage System** and **Owners** tabs contain reports for the selected storage system (VSPE1090_700032). Each tab contains a pre-defined set of workload reports.

By default, reports for the previous 7 days are displayed (the maximum). You can decrease data range as desired.

You can download individual reports as an image (PNG) or CSV data using the ≡ icon. The reports can also be downloaded in the PDF format. To download all these reports in a PDF file, click the **Download Workload Analysis Report** button.

Scheduling the Workload Analysis report

You can also schedule Workload Analysis report to get those over an email for offline usage.



Note: Workload Analysis report scheduling is currently supported only for Hitachi Enterprise Storage.

Report data for the storage systems is generated in as .xlsx and PDF files. The spreadsheet and PDF are downloaded in a zip file. Unlike chart reports in the UI:

- The spreadsheet contains maximum and average values for the storage system, owners, and LDEV performance metrics.
- The PDF contains storage system and workload summaries, cache write pending rate, and MPB utilization details. It also contains the chart reports, such as storage system read IOPS, CLPR cache utilization, and so on.

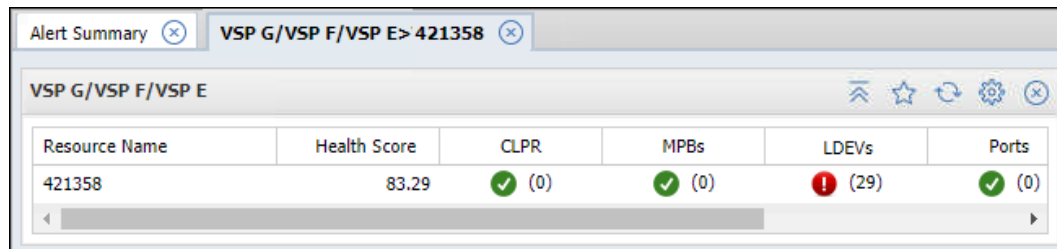
To view this report, you must schedule and then download the .xlsx file in the Reports > Schedule window:

- [Scheduling the report \(on page 40\)](#)
- [Downloading scheduled reports \(on page 44\)](#)

Analyzer detail view Dashboard view

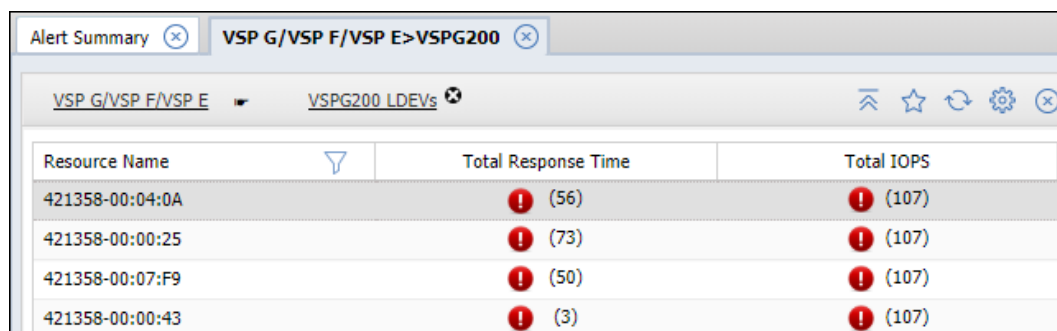
The Dashboard view shows the overall health of the monitored IT infrastructure. Analyzer detail view continuously processes incoming data and compares it with key performance indicators that are defined for each resource metric.

These conditions are continuously evaluated and depicted in a traffic light display with red (Critical), amber (Warning), and green (Normal) indicators. The dashboard displays any condition that requires immediate attention.



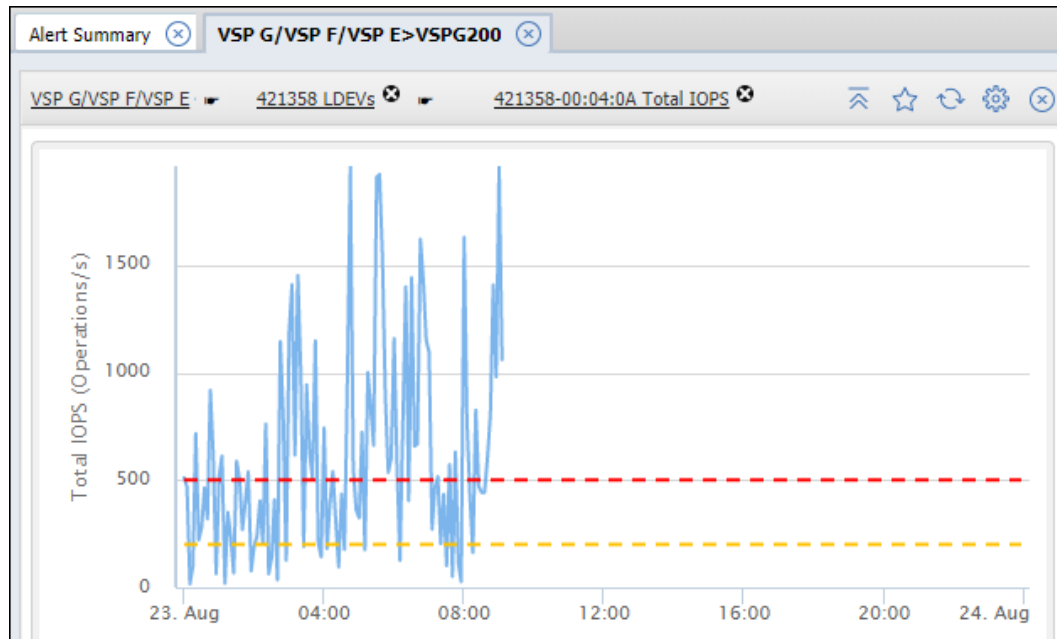
Resource Name	Health Score	CLPR	MPBs	LDEVs	Ports
421358	83.29	✓ (0)	✓ (0)	! (29)	✓ (0)

In the previous example, the dashboard shows that storage resource 421358 has violated critical thresholds. You can click the Critical icon for further details.



Resource Name	Total Response Time	Total IOPS
421358-00:04:0A	! (56)	! (107)
421358-00:00:25	! (73)	! (107)
421358-00:07:F9	! (50)	! (107)
421358-00:00:43	! (3)	! (107)

In this case, the total response time and total IOPS on various LDEVs has exceeded the critical threshold. For further details, click the Critical icon to view a graph of the metrics over time.



For example, the graph shows that the total IOPS exceeds the critical threshold.

Analyzer detail view Alerts view

The Alerts Summary tab is the default display and contains a high-level summary of all resources alerts. The Alerts view shows only the alerts for the selected node.

Alerts define conditions for critical parameters such as response time and throughput. When one or more of these conditions is violated, the information is displayed in the UI and an email notification is sent to the email recipients (and the Syslog server), enabling you to take action before users are affected.

Alert Summary		Storage Systems>Hitachi			
By Category		By Severity			
Category	Total Alerts	New Alerts	Severity	Total Alerts	New Alerts
Hosts Windows	1207	1207	Warning	1946	1946
Hitachi VSP G/VSP F/VSP E	804	804	Critical	850	850
NetApp C-Mode	406	406			
Switches Cisco FC Switch (CL)	252	252			
By Category and Severity					
Category	Severity	Total Alerts	New Alerts		
Hosts Windows	Critical	444	444		
	Warning	763	763		
Hitachi VSP G/VSP F/VSP E	Critical	0	0		
	Warning	804	804		
NetApp C-Mode	Critical	406	406		
	Warning	0	0		

An Alert notification identifies the resource and metric violating the alert condition. The following example definition triggers an alert when the Read Response Time of the pool is greater than 10 milliseconds for 10 samples of the last 30 minutes. (The last part of this definition rules out a transitory spike, ensuring the notification is worth pursuing.)

Add Alert

✓ **Alert Details :** Alert Name -> WARNING

✓ **Alert Resource :** Hitachi VSP G/VSP F/VSP E >> RAID Pool

Alert Condition

Metric:* Read Response Time (ms)

Condition:* greater than

Threshold:* ☒ Static 10 [Customize Threshold For Resources](#)
☐ Dynamic

Criteria:* When condition is met 10 samples out of 30 minutes

Alert Notification

Add Alert Cancel

You can obtain details for each alert in the Alert Violations tab by clicking the plus symbol (+) for the resource.

Duration: Latest (2020-01-20 00:00 - 2020-01-20 23:59) Options

Alert Violations

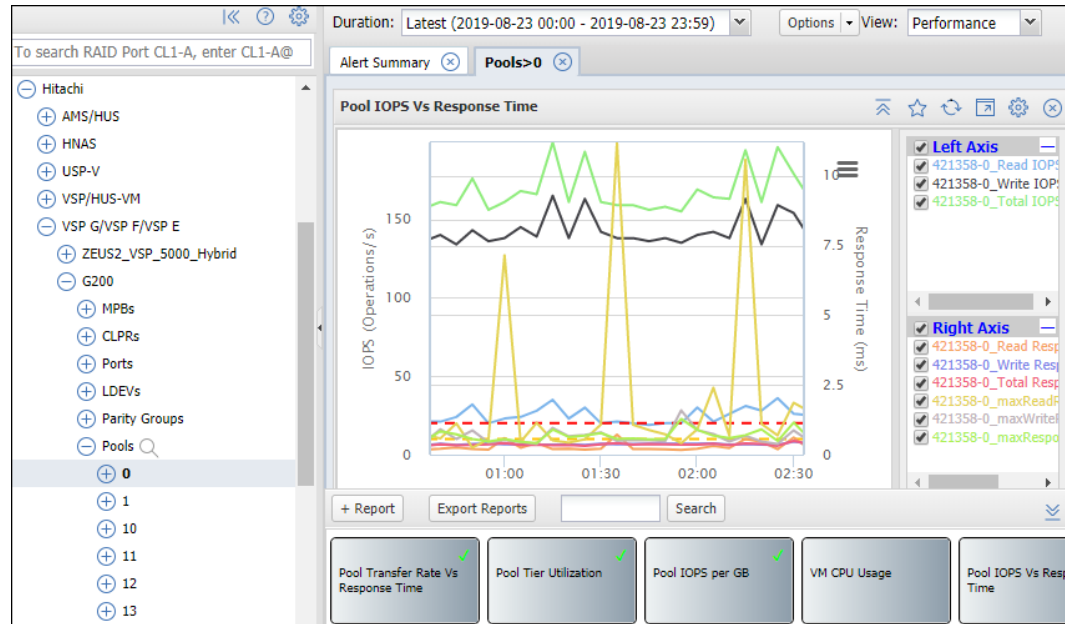
☐ Acknowledge All Refresh Filter ?

	Resource	Category	Alert Name	Severity	Triggered When	Acknowledge (New)
+	15284-0	Hitachi VSP G/VSP F/VSP E	Raid CLPR 6060	!	2020-01-20 15:41	☐
+	15284-0	Hitachi VSP G/VSP F/VSP E	Raid CLPR 6060	!	2020-01-20 15:40	☐
+	15282-0	Hitachi VSP G/VSP F/VSP E	Raid CLPR 6060	!	2020-01-20 15:40	☐
+	15284-0	Hitachi VSP G/VSP F/VSP E	Raid CLPR 6060	!	2020-01-20 15:39	☐
+	15282-0	Hitachi VSP G/VSP F/VSP E	Raid CLPR 6060	!	2020-01-20 15:39	☐
+	15284-0	Hitachi VSP G/VSP F/VSP E	Raid CLPR 6060	!	2020-01-20 15:38	☐

Analyzer detail view Reports view (Performance and Configuration)

Analyzer detail view includes a reporting facility with powerful analysis capabilities. An interactive chart helps you to view details of your report and filter the resources for a complete understanding. Each object in the tree has predefined reports. These reports cover the most significant attributes of a resource. There are two types of reports: Performance and Configuration.

Performance view



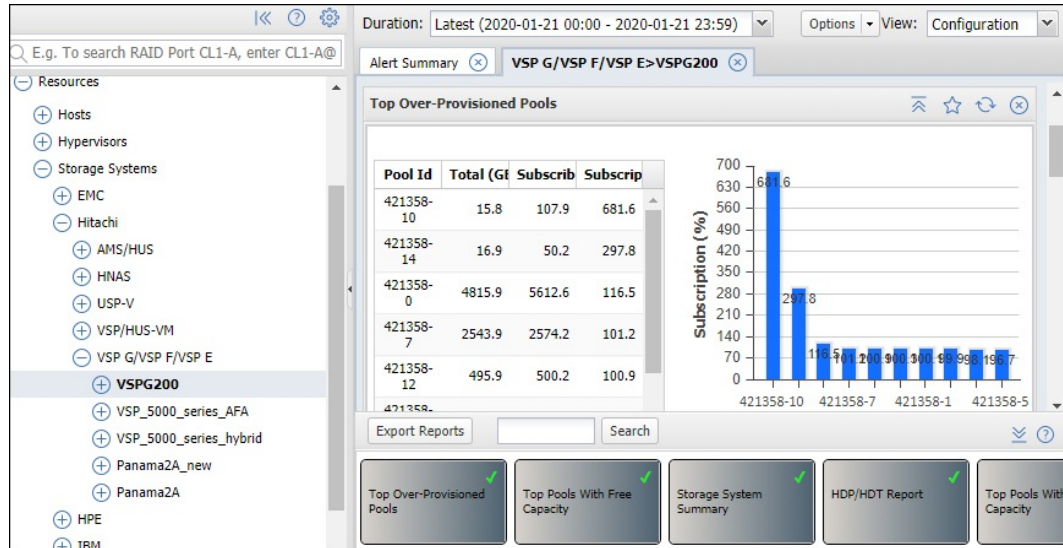
The Performance view displays data for the node selected in the tree. In this case, Pool=0 is selected and the report is Pool IOPS Vs. Response Time. This view also displays data in real-time at every one-minute level, if the real-time data option is enabled while setting the Analyzer detail view. When the real-time view report is loaded for the first time, it shows the real-time and non-real-time data; later the data is shown at every one-minute level.



Note:

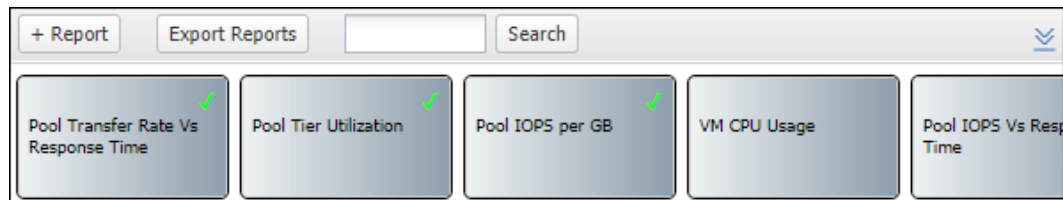
- For the Brocade switches, the same zones are displayed in all related switches in Resource Tree. However, the performance data for the switch is shown if the end port displayed in the zone belongs to that switch.
- The No data available for current view message is displayed in the performance reports when:
 - Viewing the Cache Path Usage and DKA Cache Path Usage reports for other than the following supported models: VSP F1500, VSP G1000, and VSP G1500.
 - Performance data is not being collected from the target devices.
 - Performance data for the target devices is not imported in the Analyzer detail view server.

Configuration view



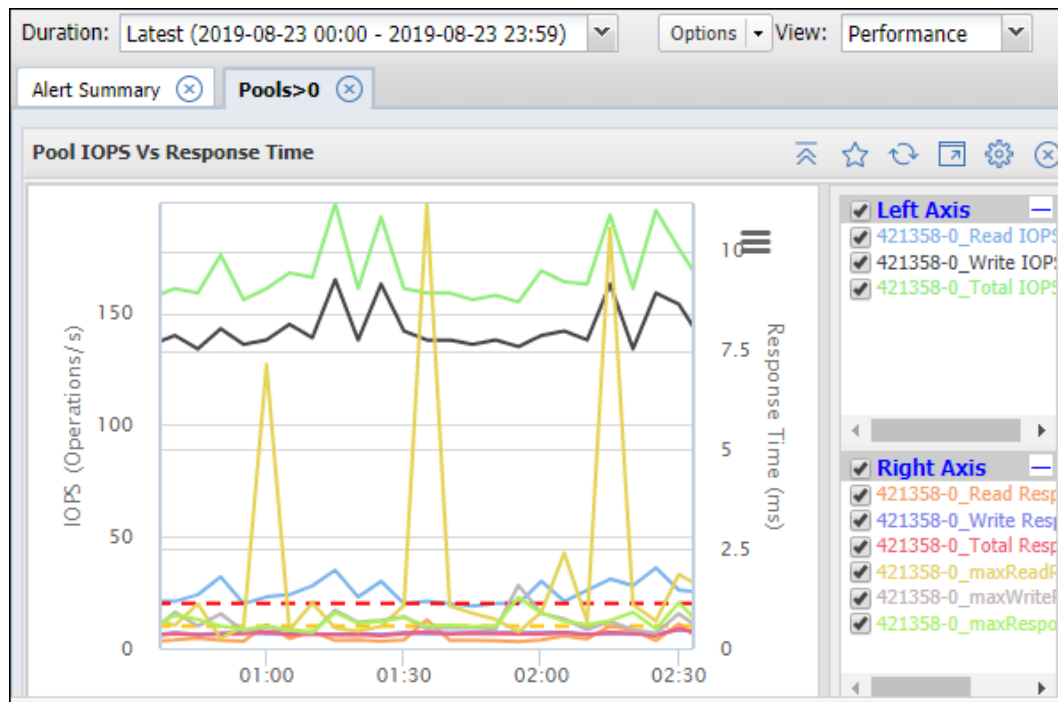
The Configuration view displays details for the resource selected in the tree. In the above example, top over-provisioned pools are displayed in a table and chart.

Reports dock



The Reports dock is available for the Configuration, Performance, and Dashboard views. The Reports dock provides the report templates. You can also create custom performance report templates in the Reports dock. You are not limited to reporting on a single resource. You can combine different resource metrics by dragging and dropping them from elsewhere in the tree.

Reports pane

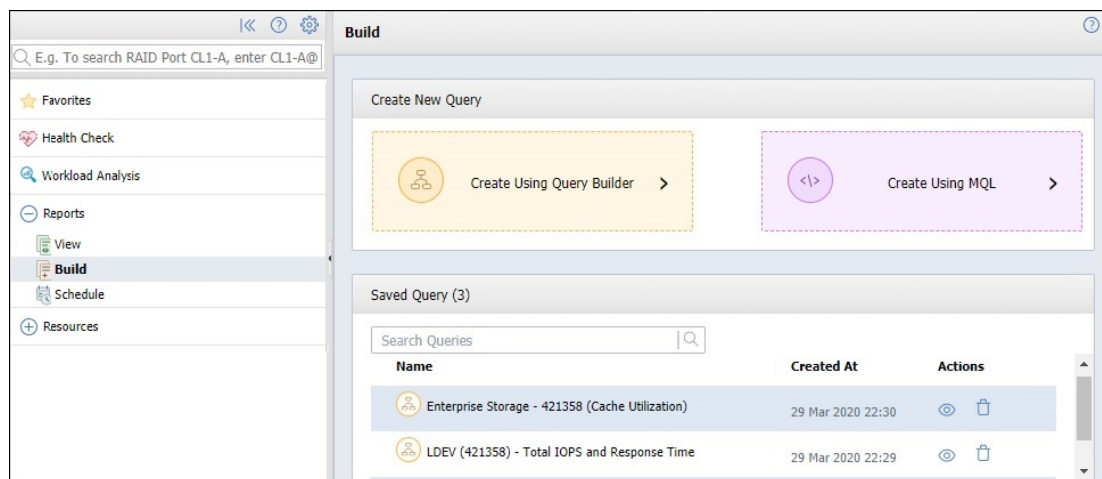


The Reports pane is available for the Configuration, Performance, and Dashboard views. You can access reports by selecting a resource in the Resource tree or clicking a report template in the Reports dock.

Analyzer detail view Report Builder

The Report Builder feature provides you the flexibility of creating your own queries and generate reports. With this feature, you can create a report of the resources and the associated metrics, which you want to monitor closely. You can also extend the built-in reports in the Analyzer detail view.

See [Creating custom reports using the Analyzer detail view Report Builder \(on page 102\)](#) for more information.



Analyzer detail view Report Scheduler

While monitoring multiple data centers, you might want to receive Health Check reports over an email for offline usage. For example, offline reports could be useful typically to check health for a specific period, or provide health status to higher management on a scheduled basis, or view the inventory report to ensure that recently-added hardware is reflected in the Analyzer detail view. You can achieve this with the Report Scheduler.

The Report Scheduler allows you to create a schedule for generating reports and delivering them in email periodically at the specified interval.

With the Report Scheduler feature, you can:

- Schedule the Health Check report to view the overall health of your data center.
- Schedule an Inventory report to view the infrastructure details of your data center.
- Schedule the Workload Analysis report to view workload information of applications and underlying resources.
- Schedule the Replication report to view relationship between virtual and physical storage systems for global-active device (GAD) pairs.
- Schedule the VSM Summary report to view configuration and performance details of the Virtual Storage Machine (VSM) in your environment.
- Set the report frequency: **One Time**, **Daily**, or **Weekly**.
- Email the scheduled report to any number of users.
- Download scheduled report from the UI.
- View existing schedules and edit them as required.

Report schedule workflow

The following is the high-level workflow to create schedule:

1. Select the report that you want to schedule.



Note:

- Currently, the Health Check, Inventory, Replication, Workload Analysis, and VSM Summary reports are supported.
- In the VSM Summary report, the used capacity reported for a VSM does not contain the used capacity of the Basic, External, and TI S-Vol (VVOL) volumes.

2. Select the target types (such as Hypervisor, Storage systems) to monitor.
3. Select the report frequency.
4. (Optional) Select recipients to receive reports by an email.
5. View the report by downloading it from the UI or accessing it through email.

Scheduling the report

You can schedule the Health Check and Inventory reports.

Procedure

1. In the left pane, click **Reports > Schedule**.
The **Schedule** window opens.
2. When you use the Report Scheduler feature for the first time, the **Schedule** section is empty. To begin, click **Create Schedule**.
3. In the **Select Report** section, do the following and click **Next**:
 - **Report Type**: Select the report type.



Note:

- A report type is only displayed if its license is registered in the Analyzer detail view except for the replication report.
- In the VSM Summary report, the used capacity reported for a VSM will not contain the used capacity of the Basic, External, and TI S-Vol (VVOL) volumes.
- The Workload Analysis report scheduling is currently supported only for Hitachi Enterprise Storage.

- **Select Target Type**: Based on the selected report type, select the target type.



Note: A target type is only displayed if its license is registered and the data is currently available in the Analyzer detail view.

For example, if you have a license for Hitachi Enterprise Storage and VMware and only Hitachi Enterprise Storage data is currently available, only **Hitachi Enterprise** appears in the **Select Target Type** list for Inventory report.

4. In the **Select Frequency** section, select the frequency and duration, and then click **Next**.

- **One Time:** Specify the date range and time to schedule the one time report.
 - The report is generated for the specific date range and the time that you provide. For example, if you select duration of 5 days, the report generation will consider the data for the selected duration.
 - The report generation for this schedule starts immediately after the schedule is created.
 - The Health Check report have a maximum duration of 7 days. The Inventory, Workload Analysis, and Replication reports have a maximum duration of 31 days.
- **Daily:** This schedule generates a daily report that includes data for the previous day. For example, if you are creating a schedule today, then the report generation will start from tomorrow at 01:00 am Analyzer detail view application time.
- **Weekly:** Specify the duration and the report generation day.
 - **Report Duration:** Select the report days duration within a week. The weekly report contains the data for the selected duration.
 - **Report Generation Day:** Select the day of the week when the report is to be generated. The report will be generated every week on specified day at 01:00 am Analyzer detail view application time.



Note:

- The following examples describe when the first schedule report generation starts:
 - If you are creating a schedule on Friday and select the report generation day as Friday, then the report generation will start from the next Friday.
 - If you are creating a schedule on Thursday and select the report generation day as Friday, then the report generation will start from the next day (Friday).
- The following examples describe whether the weekly report contains the data of the current week or previous week:
 - If the report duration is from Monday-Friday and the report generation day falls between Monday-Friday, then the report will contain the data for the previous week.
 - If the report duration is from Monday-Friday and the report generation day is Saturday or Sunday, then the report will contain the data for the current week.

5. (Optional) In the **Select Recipients** section, enter one or more email addresses to send the report over an email, and then click **Next**. If you use this option, you will receive an email as soon as the report is generated.



Note: You must configure the SMTP server details to send reports over email. Refer to the [Configuring the SMTP server for the Analyzer detail view for detail view \(on page 50\)](#).

- To add multiple email addresses, click
- To add email groups, click the **Add Email Groups** link.
- To create a new email group, click the **Add Email Groups** link, and then click **Create Email Group**. Provide the group name and email addresses. (To add multiple email addresses in a group, press **Enter**.)

6. In the **Summary** section, you can review and make changes to the schedule details before creating the schedule. Click the pencil icon to edit the details.
7. Click **Create**, and provide a name for the schedule.
8. The schedule is created and shown in the **Schedule** section. This schedule will be visible to all the users.

Schedule

Create Schedule

Showing 4/4

Search Name

Report Type

All

Frequency

All

Status

All

Name	Report Type	Frequency	Status	Updated At	Next Schedule	Actions	Download Report
Host	Health Check	Daily	Scheduled	25 Mar 2020 19:34	26 Mar 2020		
Hypervisors	Health Check	One Time	Successful	25 Mar 2020 19:36	-		
Switches	Health Check	Weekly	Scheduled	25 Mar 2020 19:37	30 Mar 2020		
Storage Systems	Health Check	Daily	Scheduled	25 Mar 2020 19:37	26 Mar 2020		

Viewing and managing report schedule

In the **Schedule** section, you can view and manage the schedule and download generated reports. By default, schedules are sorted based on the updated time (in the **Updated At** column). You can also search for a specific schedule and can apply filters:

- Search
- Report Type
- Frequency
- Status



Note: If Analyzer detail view is down for a period and restarted, the Reports Scheduler does not consider the days for which the Analyzer detail view was down. It starts generating the report from the current day.

The following table describes the Schedule section:

Column	Description
Name	Name of the schedule

Column	Description
Report Type	Report type of the schedule
Frequency	Frequency of the schedule (One Time, Daily, or Weekly)
Status	The current status of the schedule: ▪ Scheduled: The schedule is created, but not yet applicable to start the report generation. ▪ In Queue: The schedule is in the report scheduler queue ▪ In Progress: Report generation has started. You can stop the report generation by clicking the  icon. However, after you stop the report generation you cannot revert this action. For a Daily or Weekly schedule, clicking the  icon will stop the current report generation, but it will resume on the next scheduled day. ▪ Successful: The report has generated successfully. ▪ Failed: The report generation failed. For Daily and Weekly schedules, the next report generation will be attempted at the next scheduled day. ▪ Paused: The schedule is paused. For Daily and Weekly schedules, after resuming the status changes to Scheduled. ▪ Stopped: When you stop the in progress schedule.
Updated At	Time when the schedule status was updated.
Next Schedule	Day when the next scheduled report generation will start.

Column	Description
Actions	You can perform the following actions: ▪ Pause  or Resume : You can pause the daily and weekly schedules and resume as required.  Note: You cannot pause the one time schedule. After resuming a schedule, report generation will start from the next schedule day (skipping intervening days). ▪ View details : You can view the details of the schedule and edit the following details of Daily and Weekly schedule: • Add or remove the target types. • Add or remove email recipients. • Edit the Report Duration and Report Generation Day for Weekly schedule. • You can delete any schedule added by you. Users with administrator privileges can delete any schedule.
Download Report	Download the scheduled reports using the download  option. For more information, see Downloading the scheduled reports (on page 44).

Downloading scheduled reports

You can download scheduled reports from the Reports > Schedule section.

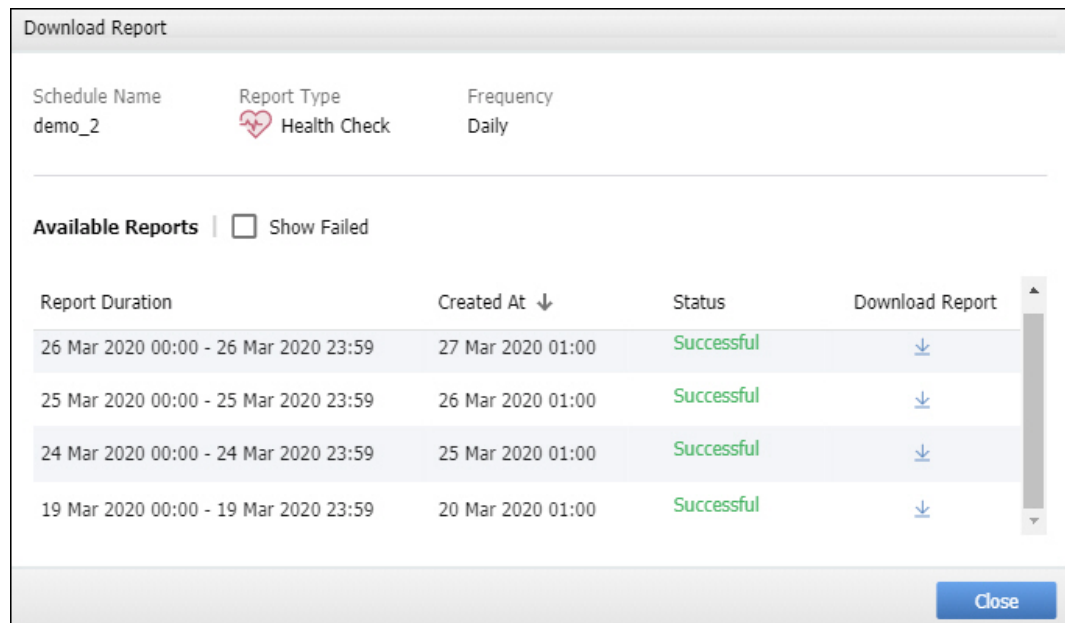
- **One Time schedule:** In the **Schedule** section, click the download  option for the schedule. A Zip file is generated that contains the report in xlsx format.

This report is available up to 8 days for download, after which the schedule entry is deleted.

- **Daily and Weekly schedule:**

1. In the **Schedule** section, click the download  option for the schedule.

The **Download Report** window lists all the generated reports based on the schedule.



2. Click the download  option for the report.

A Zip file is generated that contains the report in xlsx format.

- The daily report is available up to 8 days from the report generation day to download.
- The weekly report is available up to 35 days from the report generation day to download.

3. You can also view failed reports by selecting the **Show failed** check box.

Changing report retention

The Report Scheduler retains generated reports for specific days. However, you can change these retention days by adding the properties in a property file.

Retention depends on the frequency of the schedule.

- One Time: 8 days
- Daily: 8 days
- Weekly: 35 days

To change these values, do the following.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Stop the crond service and verify the status with these commands:

```
service crond stop
service crond status
```

3. Stop the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh stop
/usr/local/megha/bin/megha-jetty.sh status
```

4. Take a backup of custom.properties file:

```
cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
bkp_custom.properties_bkp
```

5. Open the custom.properties file:

```
/usr/local/megha/conf/custom.properties
```

6. Add the following properties with the desired retention days at the end of the custom.properties file, and save the file:

- `schedule.oneTime.export.report.retention.policy.time.in.days=15`

- `schedule.daily.export.report.retention.policy.time.in.days=10`

- `schedule.weekly.export.report.retention.policy.time.in.days=60`

7. Start the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh start
/usr/local/megha/bin/megha-jetty.sh status
```

8. Start the crond service and verify the status with these commands:

```
service crond start
service crond status
```

Chapter 2: Getting started

Follow these procedures before using Analyzer detail view.

Accessing the Analyzer detail view

You can access the Analyzer detail view UI from any supported browser.

For most Analyzer detail view operations, you can access the Analyzer detail view server from the Ops Center Analyzer More Actions menu. Certain management tasks require logging into the Analyzer detail view server as the `admin` user instead of using the More Actions menu (which logs into the server as a general user). The management tasks documented in this guide state when it is necessary to log in as the `admin` user.

Procedure

1. In your browser, enter the Analyzer detail view URL:
`https://server-IP-address:Port-Number`
(The default port for https access is 8443.)
The **Logon** window appears.
2. In the **Username** and **Password** fields, type your user name and password, and then click **Login**.

Adding detail view users

You can add local and Active Directory users in the administrator or normal user group.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the application bar, click the **Manage** menu.
3. In the **Manage** window, in the **Administration** section, click the **Manage Users** link.
4. In the **Manage Users** window, click **Add User**.
5. In the **Add User** window, select the **User Type** as `Local User` or `Active Directory User`.

The following table describes the user access rights (permissions). The access rights (permissions) are based on the administrator and normal groups assigned to a user type.

Yes indicates that the user has access rights (permissions).

No indicates that the user does not have access rights (permissions).

Group	User type	Can change Password of the following users:		Can reset password of the following users:		Can delete the following users:		Can enable strict Active Directory mode:
		Self	Other local users	Self	Other local users	Self	Other local and Active Directory Users	
Administrator	Local	Yes	No	Yes	Yes	No	Yes	No
	Active Directory	No	No	No	Yes	No	Yes	Yes
Normal	Local	Yes	No	Yes	No	No	No	No
	Active Directory	No	No	No	No	No	No	No

■ **Local User:** Provide the appropriate information in each field:

- **User ID and Password:** To log on to the Analyzer detail view and Analyzer probe. The user ID cannot include greater than and less than signs (< >), Square brackets ([]), spaces, double quotation mark ("), colon (:), and ampersand (&).
- **First Name and Last Name**
- **Email Address:** Email address of the user.
- **Group:** Select the group to which the user is to be assigned:



Note: This list is displayed only for the Analyzer detail view. The Analyzer probe supports only the administrator group.

- **Administrator:** The user with administrator rights (permissions) has access to all features of the Analyzer detail view and Analyzer probe.
- **Normal:** The user with normal rights (permissions) has access to Analyzer detail view with the following features in the **Manage** menu:
 - Authentication Token
 - Download SNMP MIB File
 - Manage Active Directory Groups (View only access)
 - Manage Email Groups
 - Manage SMTP
 - Manage SNMP
 - Manage Syslog
 - Manage Thresholds
 - Manage Users: Access to edit the email address, locale, and password.
 - Show Schema
 - Custom Reports
- **Locale:** Only U.S. English locale is supported.

- **Active Directory User:** Provide the appropriate information in each field:
 - **User ID:** You must set the User ID (with the fully qualified domain name) for an active directory in one of the following formats: The user ID cannot include greater than and less than signs (< >), Square brackets ([]), spaces, double quotation mark ("), colon (:), and ampersand (&).
 - *FQDN\user-name*
Example: corp.company\smith
 - *user-name@FQDN*
Example: smith@corp.company
 - You must use the host name as the domain controller name.
 - **Email Address:** If there is a technical problem, email is sent to that email address.
 - **Group:** Select the group to which the user is to be assigned:



Note: This list is displayed only for the Analyzer detail view. The Analyzer probe supports only the administrator group.

- **Administrator:** The user with administrator rights (permissions) has access to all the features of Analyzer detail view, except changing the password of an active directory user.
- **Normal:** The user with normal rights (permissions) has access to Analyzer detail view and the following features in the **Manage** menu:
 - Authentication Token
 - Manage Active Directory Groups (View only access)
 - Manage Email Groups
 - Manage SMTP
 - Manage Syslog
 - Manage Thresholds
 - Manage Users: Access to edit the email address and locale.
 - Show Schema
 - Custom Reports
- **Locale:** Only the U.S. English locale is supported.

6. Click **Submit**.

Configuring the SMTP server for the Analyzer detail view for detail view

You must configure the SMTP server to receive email alert notifications from detail view .



Note: The Analyzer detail view server supports the following SMTP authentication methods:

- PLAIN
- LOGIN

Before you begin

- The Analyzer detail view server supports TLS or SSL encryption for secure communication with an SMTP server. If you want to use the TLS or SSL encryption, import the TLS or SSL certificate in the Analyzer detail view server. Refer to [Importing TLS or SSL certificate for the SMTP Server \(on page 152\)](#) for more information.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the application bar, click the **Manage** menu.
3. In the **Administration** section, click the **Manage SMTP** link.
The **Manage SMTP** window opens.
4. In the **Manage SMTP** window, under **SMTP Settings**, enter the following details:
 - **Server Name:** SMTP server name
 - **Encryption Type:** SSL, TLS, or NONE



Note:

- The following communication methods are supported:
 - SSL: SMTPS
 - TLS: STARTTLS
- When you select NONE, authentication occurs if you provide the SMTP server username and password; otherwise, the email is sent without authentication.

- **Port:** SMTP server port number
 - **User:** SMTP server user name
 - **Password:** User password
5. In the **Email Settings** section, provide the following details:
 - **Server URL:** Included as part of the notification email, which notifies the recipient that the alert was received from that URL. The recipient can click the URL to view the report in Analyzer detail view.
 - **Sender Email ID:** Email account from which messages are sent to recipients.
 - **Max Size of attachment in MB:** The attachment limit for a notification is 10 MB. If the limit is exceeded, the message is sent without an attachment.
 6. Click **Send Test Email**.
The **Send test mail** window opens.
 7. In the **Receive Email ID** field, enter the recipient email account. The test message is sent to the specified email account.

8. Check the inbox to verify that the recipient has received the test email.
9. Click **Save**.

Configuring the Syslog server for detail view

You must configure the Syslog server to receive alert notifications from detail view .



Note: You cannot add the Syslog server name or Syslog server IP address twice in the system.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the application bar, click the **Manage** menu.
3. In the **Administration** section, click the **Manage Syslog** link.
The **Manage Syslog** window opens.
4. In the **Manage Syslog** window, click the **Add Syslog Server** link.
The **Add Syslog Server** window opens.
5. Type the following details:

- **Server Name:** Syslog server name or the IP address



Note: The **Server Name** field supports alphanumeric characters, hyphen (-), underscore (_), and dot (.).

- **Protocol:** TCP or UDP
- **Port:** Port number of the Syslog server

6. Click **Add**.



Note: The alert notifications are sent to the syslog server are always in the GMT time zone and do not consider the time zone that is configured on the Analyzer detail view. This is a default behavior of the Syslog server.

Editing the Syslog server settings

You can edit the protocol and port details of the Syslog server.



Note: You cannot change the Syslog server name.

Procedure

1. In the **Manage Syslog** window, in **Action**, click the **Edit** link.
The **Edit Syslog Server** window opens.
2. Edit the protocol and port details, and click **Submit**.

Configuring an SNMP Manager

You can configure the Analyzer detail view to send notifications about your storage infrastructure to the SNMP Manager.

The Analyzer detail view sends notifications in the form of traps to the SNMP Manager. The trap structure is defined in a Management Information Base (MIB) file. You can download the MIB file in the Analyzer detail view from **Manage > Download SNMP MIB File**. A zip file is downloaded, which contains separate MIB files for the SNMP versions (v1, v2c, and v3). The content of the MIB file is described in [Contents of the MIB file on the Analyzer detail view \(on page 137\)](#). The Analyzer detail view sends the performance-based alerts as described in [Setting up alerts \(on page 65\)](#).



Note: The supported SNMP versions are v1, v2c, and v3.

If you are using v3 and your SNMP Manager cannot discover the Analyzer detail view engine ID, then you must create a user with Analyzer detail view engine ID on the SNMP Manager. To obtain the Analyzer detail view engine ID, run the following command on the SNMP Manager:

```
snmpget -v <1 or 2c> -c public <ANALYZER DETAIL VIEW SERVER NAME/IP>:9191
SNMP-FRAMEWORK-MIB::snmpEngineID.0
```

Procedure

1. In the application bar, click the **Manage** menu.
2. In the **Administration** section, click **Manage SNMP**.
3. In the **Manage SNMP** window, click **Add SNMP Manager**.
4. Provide the following details:
 - **IP address or Hostname:** IP address or Hostname of the SNMP Manager.
 - **Port:** Port number from 0 to 65535 (default: 162).
5. In the **SNMP Version Settings** section, select version v1 or v2c and provide the **Community String** details. (Default: public)
6. For v3, you can choose the **Security Level**:
 - **NoAuth_NoPriv** SNMP trap messages are neither authenticated nor encrypted.
 - **Auth_NoPriv** SNMP trap messages are authenticated but not encrypted.
 - **Auth_Priv** SNMP trap messages are authenticated and encrypted.

Depending on the selected security level enter the appropriate details:

- **User Name** User name of the SNMP Manager.
- **Security Name** Security name associated with the user name.
- **Authentication Protocol** If you choose Auth_NoPriv or Auth_Priv security level, you must also select MD5 or SHA authentication protocol. (Default: MD5)
- **Authentication Password** Type the password of the authentication protocol.
- **Encryption Protocol** If you choose Auth_Priv security level, you must also select AES or DES encryption protocol. (Default: AES)
- **Encryption Password** Type the password of the encryption protocol.

7. (Optional) Specify the following advanced settings:

- **Protocol:** The default protocol is UDP and cannot be changed. If you are using SNMP version v3, then you must configure a firewall rule to allow incoming connections on UDP 9191 port.
- **Notification Type:** Trap (default) or Inform. For SNMP version v2c and v3 you can specify the notification type.
- **Trap:** The SNMP Manager does not send an acknowledgment when it receives a trap.
- **Inform:** The SNMP Manager sends an acknowledgement when it receives an inform.

If you select **Inform** you can set the following:

- **Retry count:** The number of times to retry sending a notification. (You can select between 1 to 5 retry count, the default is 1.)
- **Retry Interval:** The number of seconds to wait between retries. (You can select between 1 to 60 seconds, the default is 5 seconds.)

8. (Optional) Click **Send Test Message**, to send the test notification to the SNMP Manager.

The sample test message sent to SNMP Manager from the Analyzer detail view.

```
.1.3.6.1.4.1.116.5.63.12.2.13.0 - "Test Message to check connectivity for SNMP
Manager SNMP-Manager-IP-address or hostname"
1.3.6.1.4.1.116.5.63.12.2.16.0 - Analyzer detail view server-IP-address or
hostname
```



Note: When the value of the `sysUpTime` in the trap messages reaches to 497 days, the `sysUpTime` value resets to zero (0).

Using the Advanced Activity Monitor

The Advanced Activity Monitor (AAM) monitors the Analyzer probe server and the Analyzer detail view server and alerts you by email when the servers require attention. These alerts also include instructions on how to use the HDEBBUG shell to address the problem.

The following table describes the events for which AAM alerts are sent.

Alert Category	Analyzer detail view server	Analyzer probe server
Process monitoring	crond, syslog, HTTPS, web server, and the Analyzer detail view server (jetty) processes are not running or responding.	crond, syslog, web server, and the Analyzer probe server (jetty) processes are not running or responding.
Application status monitoring	- Data downloading and raw data processing have stopped. - Configuration and performance data import has stopped. - The alert notification and internal threads for real time and report cleaning have stopped. - The license has expired.	- Collection of configuration or performance data is delayed. - Data or probe log uploader threads are not responding. - The archive data cleaning thread is not responding. - The license has expired.
System status monitoring	- Disk, memory, or CPU usage is high. - A file system is read-only. - An excessive number of files are open. - Threads have stopped.	

About the HDEBUG shell

The HDEBUG shell helps you to troubleshoot problems that occur for Analyzer detail view, like problems for adding or using certain probes.

Alerts sent by AAM include instructions on using the HDEBUG shell to issue commands to address the issue described in the alert. For example:

```
Critical - Syslogd process is not running
```

The alert includes instructions on how to log in to the affected server, start the HDEBUG shell, and enter the necessary commands.

Configuring an SMTP server for AAM alerts on the Analyzer probe server

To receive AAM alerts for the Analyzer probe server, you must configure an SMTP server.



Note: The Analyzer probe server supports the following SMTP authentication methods:

- PLAIN
- LOGIN

Procedure

1. Log on to the Analyzer probe server through an SSH client (like putty) using the following credentials:

- **User:** megha
- **Default password:** Enter the megha user password.

2. Open the HDEBUG shell using the following command:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh
```

3. Connect as a Analyzer probe server user:

- a. Run the command: `connect --u user-name`
For example: `connect --u admin`



Note: Only the Active Directory and Local type of users can connect to the HDEBUG shell.

- b. Enter the password.

4. Run the command: `setSMTPConfig`

5. Provide the following details when prompted:

- **SMTP Server Name:** SMTP server IP address or host name
- **Encryption Type:** SSL, TLS, or NONE



Note: The following communication methods are supported:

- SSL: SMTPS
- TLS: STARTTLS

- **SMTP Port:** SMTP server port
- **SMTP Username:** SMTP username
- **SMTP Password:** Password of the SMTP user
- **Sender Email ID:** Email account from which messages are sent to recipients.
- (Optional) **Max Size of Attachment:** You can ignore this because AAM currently does not support attachment in email.

6. By default, AAM also sends email alerts to admin users configured in the Analyzer probe server UI. To override this setting, run the following command:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh setAAMConfig --key  
aam.email.user --value comma-separated-email-addresses
```

Configuring an SMTP server for AAM alerts on the Analyzer detail view server

To receive AAM alerts for the Analyzer detail view server, you must configure an SMTP server.

**Note:**

- The Analyzer detail view server supports the following SMTP authentication methods:
 - PLAIN
 - LOGIN
- The following communication methods are supported for SSL and TLS encryption types:
 - SSL: SMTPS
 - TLS: STARTTLS

Procedure

1. Log on to the Analyzer detail view server UI and configure the SMTP server. See "Configuring the SMTP server" in the online help for more information.
2. By default, AAM also sends email alerts to admin users configured in the Analyzer detail view server UI. To override this setting, do the following:
 - a. Log on to the Analyzer detail view server through an SSH client (like putty) using the following credentials:

- User: megha
- Default password: Enter the megha user password.

- b. Run the following command:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh setAAMConfig --key
aam.email.user --value comma-separated-email-addresses-or-
email-groups
```



Note: Email groups are configured in the Analyzer detail view server UI.

Using System Diagnostics

System Diagnostics gathers functional information and operating statistics for the Analyzer detail view server and Analyzer probe server. This includes resource consumption by system-level processes and Analyzer detail view server component activities (such as the collection and importing of data). You can access this information from System Diagnostics in the Analyzer detail view UI.

These reports can be used with the help of Customer Support to troubleshoot server-level problems. The following table describes the processes and activities monitored by System Diagnostics.

Alert Category	Analyzer detail view server	Analyzer probe server
Processes	Jetty and JVM, AAM, HTTP proxy, Apache Kafka, Redis Labs open source Redis, and System Diagnostics.	Jetty and JVM, AAM, and System Diagnostics.
Application activities	▪ Alert notification ▪ Batch import post processing ▪ Data downloading ▪ Data importing ▪ Raw data processing ▪ Report cleaning	▪ Archived data cleaning ▪ Probe data collection ▪ Data uploading ▪ File monitoring ▪ Logs uploading ▪ Data upload monitoring
Host (on which Analyzer detail view server and Analyzer probe server are installed)	CPU, memory, disk, network, and file system statistics	

Viewing System Diagnostics

Procedure

1. In the application bar, click the **Launch System Diagnostics** () icon. System Diagnostics opens in a separate browser tab.
2. Expand the tree to view the reports of the Analyzer probe server or Analyzer detail view server.



Note: You can view the performance of all those Analyzer probe servers that are sending data to a Analyzer detail view server.

3. Additionally, you can do the following:
 - Click the **View** list to choose configuration or performance details of the node.
 - Click the **Duration** list to change the diagnostics duration.

Chapter 3: Configuring the Analyzer detail view dashboard

The dashboard summarizes the status of the selected resource with a series of visual indicators. You can choose indicators to display and configure the thresholds that define them. The summary is displayed in the Dashboard view.

Understanding detail view indicators

You can set the detail view Dashboard view to show traffic light indicators or a heat map.

To view the details of a violation, click the indicator icon.

The detail view dashboard dock is available on every node in the resource tree, and it contains the dashboard widgets from all of the subnodes. You can view the indicators added by the other users, and you can select these indicators to appear on the dashboard.

Indicator view

The Indicator view provides an overall score of each resource, along with the health assessment of its components using traffic light indicators. In the Indicator view, the health score is expressed as a percent value.

In addition to the high-level resource, each of its components is assigned a score and an indicator. The score is the total number of threshold violations. You can hover over the score to view details of the Critical and Warning threshold violations.

The indicator for each component is determined by the proportion of critical and warning threshold violations for each component. The Critical threshold violations have a greater (negative) effect on the Indicator than Warning threshold violations.

At a high level, the indicators represent the following:

- **Green:** Represents a score above 70%.
Overall, the resource is healthy. The resource and its components rarely violate Critical or Warning thresholds.
- **Amber:** Represents a score above 50% but below 70%.
Indicates the resource is reasonably healthy but the user is cautioned to monitor this resource closely. The resource and its components occasionally violate Critical or Warning thresholds.
- **Red:** Represents a score below 50%.
Indicates that the resource is not healthy and might require immediate attention. The resource and its components frequently violate Critical or Warning thresholds.

The following factors influence the indicator scores:

- The frequency of thresholds violation. A large number of thresholds leads to a lower score. The number of Critical threshold violations affects the indicator score more than the number of Warning threshold violations.
- The intensity of the threshold violations is the magnitude of the violation each time it occurs. A violation of a Critical or Warning threshold by a greater margin has a higher effect on the score.

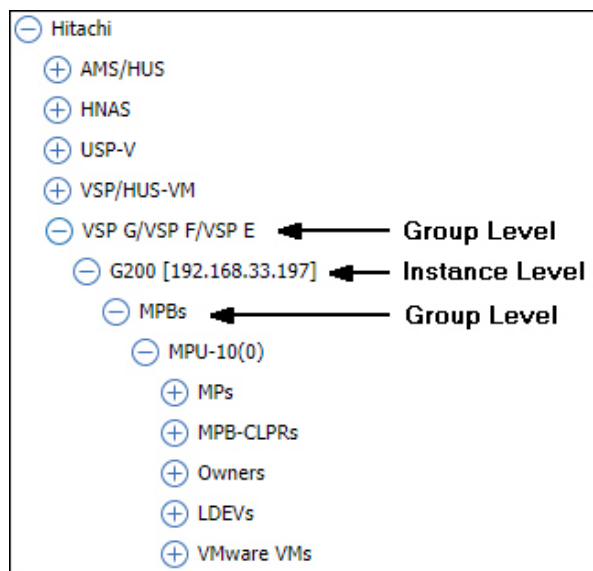
Heat map view

The heat map view displays resource health using a miniature graph of any violations of critical and warning thresholds. The values in this view (except for the display) are equal to those in the Indicators view.

Adding detail viewdashboard indicators

You can create custom indicators and specify criteria like resource, metrics, and thresholds at the Group level node in the resource tree.

Example



Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the detail view Dashboard view, click  on the dashboard bar.

The **Manage Indicators** window opens. The default indicators are disabled (and cannot be removed), but you can use the **Show** option to control which indicators are displayed.

Show	Delete	Name	Resource Type	Criteria
☒		Indicator 1	RAID Storage	Cache Usage (MB): Cache Usage MB (C > 50.0 : W > :)
☒		CLPR	RAID CLPR	CHA Cache Path Usage Rate (%): CHA Cache Path Usage Rate (C > 1)
☒		MPBs	RAID MPB	Write Pending Rate (%): CLPR_WritePendingRate (C > 40.0)
☒		LDEVs	RAID LDEV	Utilization (%): Utilization (C > 70.0 : W > 40.0)
☒		Ports	RAID Port	Total Response Time (ms): TotalResponseTime (C > 20.0 : W)
☒		Pools	RAID Pool	Total IOPS (Operations/s): TotalIOPS (C > 500.0 : W > 200.0)
☒		Parity Groups	RAID Parity Group	Transfer Rate (KB/s): Ports_TransferRate (C > 800000.0)
☒				Total IOPS (Operations/s): Ports_TotalIOPS (C > 30000.0 : W)
☒				Total Response Time (ms): TotalResponseTime (C > 20.0 : W)
☒				Utilization (%): Utilization (C > 70.0 : W > 40.0)



Note: If you click on an Instance level node (rather than the Group), the window is named **View Indicators** and all the buttons are disabled except **Close**.

3. To add additional indicators, click **Add Indicator**.
4. In the **Add Indicator** window, enter the following details:
 - **Name:** A unique name for the specific target. This appears as a column name on the dashboard.
 - **Selected Node:** Shows the node to which indicators are added.
 - **Select Resource:** Select a resource from the list to view all the subnodes.
 - **Select Subpath:** Select one or more subpaths. In the example, LDEVs is one of the subnodes of VSP G/VSP F/VSP E node. However, the LDEV (source) is connected to the VSP G/VSP F/VSP E (target) through multiple paths in the subtree of the VSP G/VSP F/VSP E node. In the **Select Subpaths** box, list all such paths.
 - **Select Metric(s):** Choose the metrics, and then select from the list of Indicator Thresholds. If no thresholds are defined, you can create new ones by selecting **Add new threshold**.

Exporting, importing, and resetting detail view dashboard indicator thresholds

You can export indicator thresholds from one Analyzer detail view and import them to other Analyzer detail view for consistency. You cannot view or edit these thresholds values outside of Analyzer detail view. You can also reset the thresholds to factory settings.

Procedure

1. Select **Tools > Ops Center Analyzer detail view** to start the detail view GUI.
2. In the application bar, click the **Manage** menu.
3. In the **Administration** section, click the **Manage Thresholds** link.
4. In the **Manage Thresholds** window, click the **Configured Thresholds** link.
The **Configured Thresholds** window opens and lists all the configured thresholds on the server. All columns except **Warning** and **Critical** have filters.
5. Click the **Export** link.
The export file is encrypted with the name of `ExportedThresholds.enc` by default. (Any filtered columns are exported as well.)
6. To import a thresholds file, click the **Import** link.
7. Click **Select File** to browse to the threshold export file, and click **Upload**.
The **Import threshold file information** window displays details such as Analyzer detail view version, URL, and supported probe list, for which you are importing the thresholds.
8. Click **Import**.
The configured thresholds table is updated with the imported thresholds.
9. Click the **Reset Defaults** link to reset the threshold indicators to the factory default settings.
10. Click **Yes**, to confirm your choice.
This restores the default thresholds and updates the display.

Editing and deleting detail view dashboard indicators

You remove detail view dashboard indicators and edit thresholds. The edit and delete options are available at the Group level node.

**Note:**

- You cannot edit the indicators added by other users. However, a user with administrator rights (permissions) can edit the indicators added by other administrators and normal users.
- You cannot delete the default indicators.
- You cannot delete indicators added by other users.
- The Delete icon is disabled for indicators that are in use.
- Users with administrator privileges can delete the indicators added by administrators and normal users.

Procedure

1. Select **Tools > Ops Center Analyzer detail view** to start the detail view GUI.
2. In the Dashboard view, choose a resource from the tree.
A tab for the resource opens with a list of indicators. (Default indicators are shaded and cannot be changed.)
3. Click  in the resource tab.
The **Manage Indicators** window opens.

Show	Delete	Name	Resource Type	Criteria
☒		Indicator 1	RAID Storage	Cache Usage (MB): Cache Usage MB (C > 50.0 : W > :)
☒		CLPR	RAID CLPR	CHA Cache Path Usage Rate (%): CHA Cache Path Usage Rate (C > 1)
☒		MPBs	RAID MPB	Write Pending Rate (%): CLPR_WritePendingRate (C > 40.0)
☒		LDEVs	RAID LDEV	Utilization (%): Utilization (C > 70.0 : W > 40.0)
☒		Ports	RAID Port	Total Response Time (ms): TotalResponseTime (C > 20.0 : W)
☒		Pools	RAID Pool	Total IOPS (Operations/s): TotalIOPS (C > 500.0 : W > 200.0)
☒		Parity Groups	RAID Parity Group	Transfer Rate (KB/s): Ports_TransferRate (C > 800000.0)
☒				Total IOPS (Operations/s): Ports_TotalIOPS (C > 30000.0 : W)
☒				Total Response Time (ms): TotalResponseTime (C > 20.0 : W)
☒				Utilization (%): Utilization (C > 70.0 : W > 40.0)

4. You can select a threshold for an indicator from the list, or delete an indicator by clicking the **Delete** icon.
5. Click **Save** when your changes are complete.

Customizing detail view dashboard indicator thresholds

You can define custom thresholds for Analyzer detail view dashboard resource indicators from the Manage menu. The thresholds that you set in this window appear in the Indicator Thresholds menu of the Add Indicator window.

Dynamic thresholds

Dynamic thresholds are supported for certain devices. You can add the threshold on the storage port throughput based on the speed of the switch port that the storage port is connected to. Analyzer detail view currently supports the dynamic thresholds for the following probes, resource types, and metrics.

Probe	Resource type	Metric
Hitachi Enterprise Storage	RAID Port	Transfer Rate
EMC VMAX	VMAX Port	MBps Ops

Procedure

1. Select **Tools > Ops Center Analyzer detail view** to start the detail view GUI.
2. In the application bar, click the **Manage** menu.

3. In the **Administration** section, click the **Manage Thresholds** link.
The **Manage Thresholds** window opens.
4. In the **Manage Thresholds** window, supply the following information:
 - **Select Probe:** Select the probe from the list.
 - **Select Resource Type:** Select the resource from the list.
 - **Select Metric:** Select the metrics for the selected probe and resource type.
 - **Add Indicator Thresholds:** Click **Add Thresholds** and type the label for the threshold, and then set the warning and critical thresholds as follows:
 - a. Type the threshold name and set the threshold value.
 - b. Configure **Advanced options** to set threshold direction (Forward or Reverse):
 - For **Forward Threshold**, the critical threshold should be greater than warning threshold. In this case, the threshold is violated when the metric value exceeds the defined threshold. By default, the threshold direction is **Forward**.
 - For **Reverse Threshold**, the warning threshold should be greater than critical threshold. In this case, the threshold is violated when the metric value is less than the defined threshold. Reverse direction thresholds are useful when evaluating metrics like Read Hit for VMAX Volume or Cache Usage. If the Read Hit rate falls below the threshold, the cache is underutilized and performance suffers.

For devices that support dynamic thresholds, the following additional options are displayed:

- **Specify Dynamic Threshold Value:** Select to specify a dynamic threshold value.
 - **Select Resource Path:** Select the appropriate switch port path.
 - **Select Attribute:** Select the attribute and provide the Warning and Critical threshold values (percentage).
5. Click **Save**.

Chapter 4: Setting up Analyzer detail view alerts

Analyzer detail view classifies metrics into two types: configuration and performance. Configuration metrics change infrequently, and include resource Status, Capacity, and so on. Performance metrics are more dynamic such as IOPS, response time, and so on.

You can set various alert conditions for configuration and performance metrics. When these conditions are met, a notification can be sent by email, SNMP or a Syslog server.

Adding detail view alerts

You can set alerts in detail view and configure notifications for them.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the application bar area, click the **Alerts** list and select **Add Alert**.
3. In the **Alerts Details** section, enter the following details:
 - **Name:** A unique name with maximum length of 100 characters. (Alert name cannot contain special characters except underscore and space.)
 - **Severity:** Severity level - Critical is red and Warning is amber.
4. In the **Alert Resource** section, enter the following details:
 - **Select:** Select the target to add the alert.
 - **Choose:** Select one or more target instances.
 - **Include future instances:** Automatically apply the alert to future target instances. (This option is only available if all target instances are selected.)
 - **Create Alerts on:** Select the resource for which you want to set the alert.
 - **For Instance(s):** Select the resource instance.



Note: The resource instances can be filtered based on certain criteria. For example, the disk type is displayed for `RAID Pool Tier` resource. You can filter the resource instances using the filter option (disk type) and then set alerts for the filtered resources. You can also choose to skip resource instances from the filtered list.

 - **Include future instances:** Automatically include any future resource instances. (This option is only available if all resource instances are selected.)
5. In the **Alert Condition** section, you can set alert condition on performance and configuration metrics:

	▼
Configuration	▲
Allocated Capacity (GB)	
Cache Size (MB)	
Capacity (GB)	
Data Reduction Ratio	
FMD Compression Ratio	
FMD Pattern Matching Ratio	
Unallocated Capacity (GB)	
Performance	
CHA Cache Path Usage Rate (%)	
Cache Usage (MB)	
Cache Utilization (%)	
DKA Cache Path Usage Rate (%)	

When adding an alert condition, you can define the static threshold for all metrics listed in the **Metric** list. You can also define the dynamic threshold for a few metrics. Analyzer detail view analyzes the data patterns for the last 7 days and automatically calculates a dynamic threshold each day based on a formula. The alerts are generated when the dynamic threshold is violated. Currently, dynamic thresholds are supported for a few Hitachi Block Storage configuration and performance metrics. Refer to the *Hitachi Analyzer Detail View Metrics Reference Guide* for the list of metrics that support dynamic threshold. See [Understanding dynamic thresholds \(on page 72\)](#) for more information.

- To set up an alert condition for configuration metrics, enter the following details:

- **Metric:** Select the configuration metric.



Note: If a resource does not have a configuration metric for alerting, it is not displayed in the list.

- **Condition:** Select the condition type. Metrics with numeric values use **greater than**, **between**, and **less than**. Metrics with string values use the **having** condition.



Note:

- Under certain circumstances, Analyzer detail view cannot identify whether a metric is a numeric or string value. When this occurs, all condition types are listed. To select the proper condition, you must know whether the metric is a numeric value or a string. You can find the value by running the query in **Report Builder**. See, [Identifying the metric value \(on page 77\)](#).
- Dynamic thresholds only support the **greater than** and **less than** conditions.

- **Threshold:** If a metric supports dynamic thresholds, you can choose whether you want to define a static or dynamic threshold.

- **Static threshold:** Type or select a static threshold value.

(Certain metrics with string values include predefined thresholds.) The value set for the **having** condition is saved and is available for other users.

The threshold value specified in this field applies to all the selected resource instances.



Note: The **having** condition supports alphanumeric characters, hyphen (-), underscore (_), comma (,), colon (:), at (@), slash (/), dot (.), and space.

- **Customize Threshold For Resources:** Click this link to customize the value for a specific resource instance.

The **Customize Threshold for Resources** window is displayed. The instances selected in the **Alert Resource** section are displayed.

- Select the instances for which you want to customize the threshold. You can also filter the instances based on criteria, such as disk type.
- In the **Set Custom Threshold** field, enter a value and then click **Update**. The threshold value is updated for the selected instances.
- Click **OK**.

- **Dynamic threshold:** The dynamic threshold is derived by adding the values of Daily Moving Average (DMA) and Standard Deviation (SD). Analyzer detail view uses last 7 days data to calculate the DMA and SD values. Based on DMA and SD values, the dynamic threshold is determined everyday when a day is changed (as per Analyzer detail view application time zone). You can select one of the following options:

- 7 DMA + or - 1 SD
- 7 DMA + or - 2 SD
- 7 DMA + or - 3 SD



Note: Depending on the selection in the **Condition** field, the + (plus) or - (minus) SD is listed. For greater than, the "DMA + SD" options are listed. For less than, the "DMA - SD" options are listed.

SD is calculated by applying a formula. 1 SD is a value derived from a formula. 2 SD and 3 SD is the value of 1 SD multiplied by 2 and 3, respectively.

For example, assume the DMA value is 20 and SD value is 10. The calculation will be as follows:

- 7 DMA + 1 SD = 30
- 7 DMA + 2 SD = 40
- 7 DMA + 3 SD = 50

You can define one of the above dynamic thresholds according to your needs. For example, you might want to use the 7 DMA + 1 SD and 7 DMA + 2 SD thresholds for the alert violation in normal cases. If you want to identify a suspicious activity (like a malware attack), defining 7 DMA + 3 SD as a threshold might be more appropriate in which the threshold is continuously violated for a significant duration.



Note: Dynamic thresholds cannot be defined using REST API.

- To set up the alert condition for performance metrics, enter the following details:
 - **Metric:** Select the performance metric.
 - **Condition:** Select the condition type: **greater than**, **between**, or **less than**.



Note: Dynamic thresholds only support the **greater than** and **less than** conditions.

- **Threshold:** If a metric supports dynamic thresholds, you can choose whether you want to define a static or dynamic threshold.

- **Static threshold:** Type the threshold value.

The threshold value specified in this field applies to all resources selected.

- **Customize Threshold For Resources:** Click to customize the value for a specific resource instance.

The **Customize Threshold for Resources** window is displayed along with the instances selected in the **Alert Resource** section.

- Select the instances you want to customize. You can also filter the instances based on criteria, such as disk type.
- In the **Set Custom Threshold** field, enter a value and then click **Update**. The threshold value is updated for the selected instances.
- Click **OK**.

- **Dynamic threshold:** The dynamic threshold is derived by adding the values of Daily Moving Average (DMA) and Standard Deviation (SD). Analyzer detail view uses last 7 days data to calculate the DMA and SD values. Based on DMA and SD values, the dynamic threshold is determined everyday when a day is changed (as per Analyzer detail view application time zone). You can select one of the following options:

- 7 DMA + or - 1 SD
- 7 DMA + or - 2 SD
- 7 DMA + or - 3 SD



Note: Depending on the selection in the **Condition** field, the + (plus) or - (minus) SD is listed. For greater than, the "DMA + SD" options are listed. For less than, the "DMA - SD" options are listed.

SD is calculated by applying a formula. 1 SD is a value derived from a formula. 2 SD and 3 SD is the value of 1 SD multiplied by 2 and 3, respectively.

For example, assume the DMA value is 20 and SD value is 10. The calculation will be as follows:

- $7 \text{ DMA} + 1 \text{ SD} = 30$
- $7 \text{ DMA} + 2 \text{ SD} = 40$
- $7 \text{ DMA} + 3 \text{ SD} = 50$

You can define one of the above dynamic thresholds according to your needs. For example, you might want to use the 7 DMA + 1 SD and 7 DMA + 2 SD thresholds for the alert violation in normal cases. If you want to identify a

suspicious activity (like a malware attack), defining $7 \text{ DMA} + 3 \text{ SD}$ as a threshold might be more appropriate in which the threshold is continuously violated for a significant duration.



Note: Dynamic thresholds cannot be defined using REST API.

- **Criteria:** Select the criteria. (The maximum value for minutes is 60). It is important to set an appropriate criteria. For example, for Dynamic threshold, if you set the criteria as 1 sample of 30 minutes, an alert will be generated for each violation and you might receive too many alert notifications. Instead, you can choose the criteria for a significant number of data samples and duration. Suppose data granularity is one minute and you set the criteria as 25 samples out of 30 minutes. So, at least 30 data points out of 30 minutes are checked and an alert is generated when 25 data points exceed the threshold. It helps you to understand that something is not normal for a significant duration (in this case it is 25 out of 30 minutes).

To select the proper alert criteria you must know the data collection interval of the metric as described in [Identifying the collection interval \(on page 73\)](#).



Note: If you want to add alerts for metrics with a data collection interval exceeding 60 minutes, you must configure the data collection interval for these metrics at least 60 minutes on the RAID Agent.

- **Monitor Between:** Select the monitoring time. The alert monitoring window is based on UTC timezone. If applicable, also consider the Daylight Saving Time. For example, if the Analyzer detail view application timezone is set to Pacific Time (GMT-08:00) and you want to add alert for time window 9:00 AM to 7:00 PM, then set alert monitoring window as 05:00 PM to 03:00 AM.

6. In the **Alert Notification** section, click the **Email**, **Syslog**, or **SNMP** tab and provide the following details:
 - **Email:** Select the email groups to which you want to send the notification, or type the individual email address. You can choose any of the following options:
 - **Each alert violation:** Sends a notification on every alert.
 - **Hourly or Daily:** Sends notification hourly or daily.
 - **The first alert violation:** Sends the first violation alert and suppresses subsequent alert notifications when alert violations happen for an extended period. Sends the second notification when the alert condition is ended.

 **Note:** You can add email groups in **Manage > Manage Email groups** and the email address in **Manage > Manage SMTP**.

 - **Syslog server:** Select the Syslog server.

 **Note:** You can configure the Syslog server in **Manage > Manage Syslog**.

 - **SNMP Manager:** Select the SNMP Manager.

 **Note:**

 - You can configure the SNMP Manager in **Manage > Manage SNMP**.
 - If you select SNMP Manager, alert violations on the real-time data are not sent to the SNMP Manager.
7. Click **Add Alert**.

Understanding dynamic thresholds

An alert is generated when a threshold is exceeded. You can define a static threshold or dynamic threshold. To define a static threshold, you need to identify the workload. Because storage systems serve multiple applications and each application is managed by a different team, it becomes difficult for a storage administrator to identify an appropriate threshold for a resource.

Dynamic thresholds help you to address this challenge. Analyzer detail view utilizes historical data to determine a dynamic threshold by comparing the current values of the metric. It uses "Day Moving Average (DMA)" and "Standard Deviation (SD)" for the last 7 days to determine the dynamic threshold by comparing dynamic threshold against the current day's values for the selected metric.

You can set the following dynamic threshold options when adding an alert:

- 7 DMA + 1 SD, or 7 DMA + 2 SD, or 7 DMA + 3 SD (if you have selected the greater than condition)
- 7 DMA - 1 SD, or 7 DMA - 2 SD, or 7 DMA - 3 SD (if you have selected the less than condition)

For a normal data set, the values within 1 SD of the mean account for about 68% of the data set, while within 2 SDs and 3 SDs of the mean account for about 95% and 99.7% , respectively. So if you select 1 SD, then 32 % of the data points can be higher as 1 SD covers 68% data set. Similarly, for 2 SD and 3 SD thresholds, 5 % and 0.3 % data points can be higher, respectively. Set the threshold carefully based on your requirement and define the appropriate (m/n) criteria in the Criteria field. For example, if you define the criteria as 1 sample out of 30 minutes, an alert will be generated for each violation and you might receive too many alert notifications. Instead, choose the criteria for significant number of data samples for a duration. Suppose data granularity is one minute and you set the criteria as 25 samples out of 30 minutes. So, at least 30 data points out of 30 minutes are checked and an alert is generated when 25 data points exceed the threshold. It helps you to understand that something is not normal for a significant duration (in this case it is 25 out of 30 minutes).

DMA and SD values are calculated based on the historical data. For example, the DMA and SD values for storage IOPS for the last 7 days are 8000 and 2000, respectively. In this case, the dynamic threshold values for 7 DMA + 1 SD, 7 DMA + 2 SD and 7 DMA + 3 SD will be 10000, 12000 and 14000, respectively. Here, the 1 SD threshold value (10000) is 25 % higher than the 7 DMA value (8000). And 2 SD and 3 SD values are 50 % and 75 % higher than the 7 DMA value. So, you can use the thresholds 1 SD and 2 SD for the alert violation in normal cases. If you want to identify a suspicious activity (like, a malware attack), you can use the 7 DMA + 3 SD as a threshold in which current data points are continuously violating the 7 DMA + 3 SD threshold for a significant time.

The dynamic threshold value is determined everyday when a day is changed (as per Analyzer detail view application time zone).

Currently, dynamic thresholds only support a few Hitachi Block Storage configuration and performance metrics. Refer to *Hitachi Analyzer Detail View Metrics Reference Guide* for the list of supported metrics.



Note: Dynamic thresholds cannot be defined using REST API.

Identifying the collection interval

When setting up an alert on the resource, you must know the data collection interval of its metrics, because the criteria are set based on the data collection interval.

You can set an alert for a metric based on the number of samples for a multiple of the collection interval. For example, if the data collection interval of a particular metric is 5 minutes, you can set alert with a criteria of 1 sample out of 5 minutes, 2 samples out of 10 minutes, 1 samples out of 10 minutes, and so on.

Criteria:*
When condition is met

samples out of

minutes

To identify the data collection interval of a particular metric, do the following:

Procedure

1. In the left pane, go to **Reports > Build**.

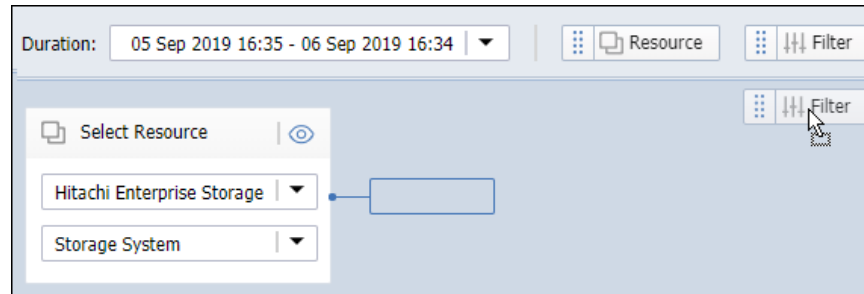
2. Click the **Create Using Query Builder** option.
3. In the **Create Using Query Builder** window, let's identify the data collection interval for the Total IOPS metric of the LDEV resource that belongs to the Hitachi Storage System serial number 421358.

- a. Select the **Resource Group** and **Resource** that you want to query.

In this example, we will select the **Hitachi Enterprise Storage** resource group and the **Storage System** resource.

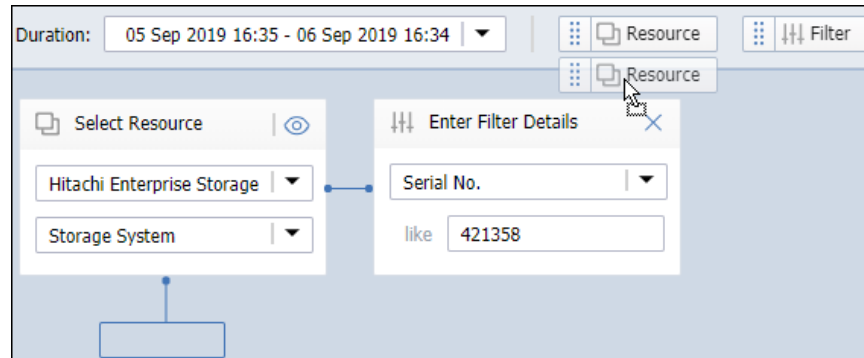
After selecting the resource group and resource, the **Resource**, and **Filter** options are enabled and a message to drag and drop the Filter or Resource is displayed.

- b. To add the filter, drag the **Filter** icon as follows:

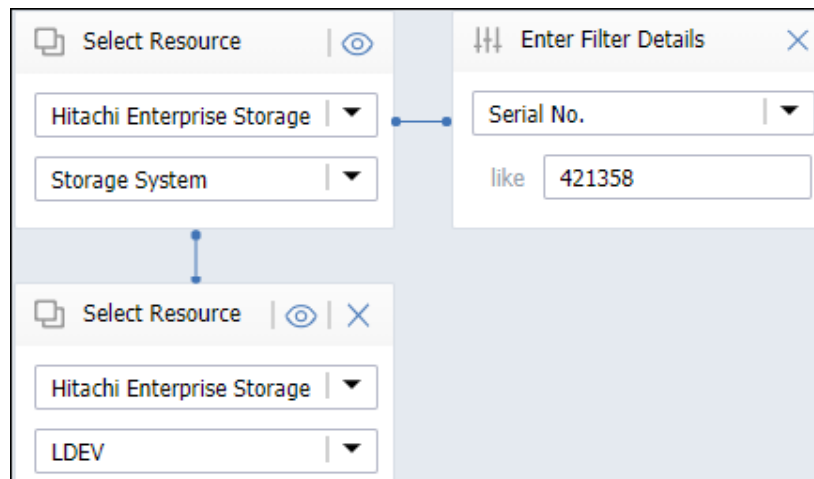


The **Enter Filter Details** box is added next to the **Select Resource** box.

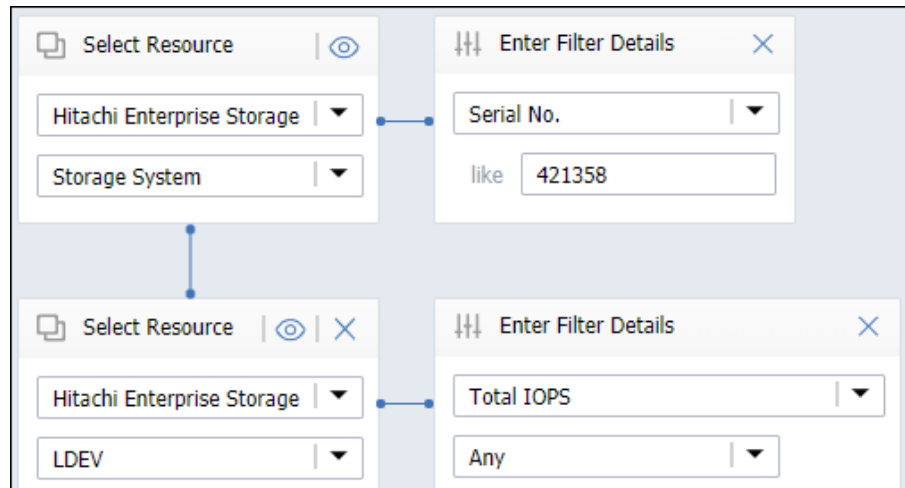
- c. Select the **Filter**. Metrics corresponding to the selected resource are listed. You may have added multiple Hitachi Enterprise Storage system probes. So, select the **Serial Number** metric and then enter 421358 in the **like** box.
- d. To find the collection interval for the Total IOPS metric of the LDEV resource, you must add the LDEV resource. Drag the **Resource** icon as follows:



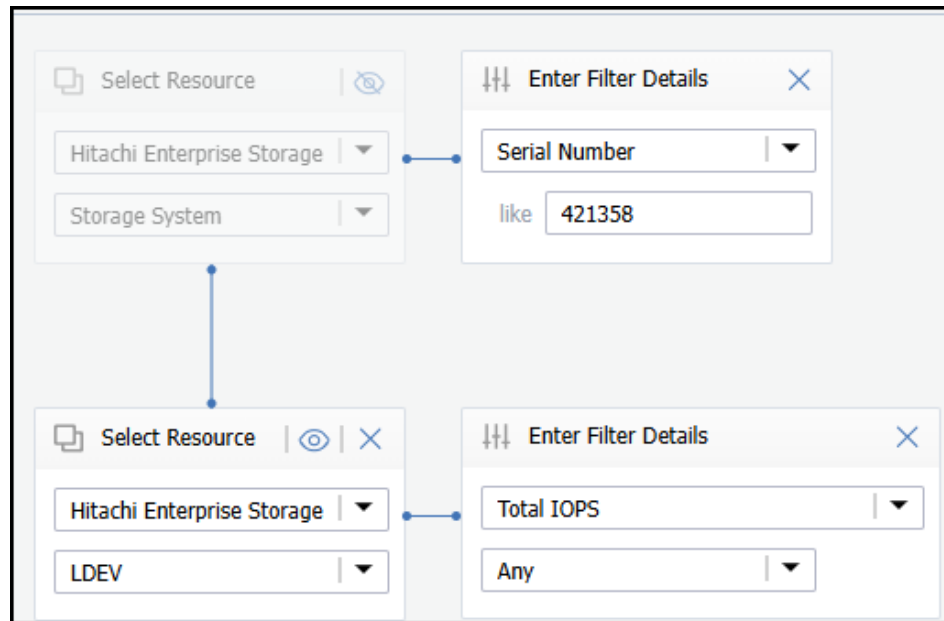
- e. Select the **Hitachi Enterprise Storage** resource group and **LDEV** resource.



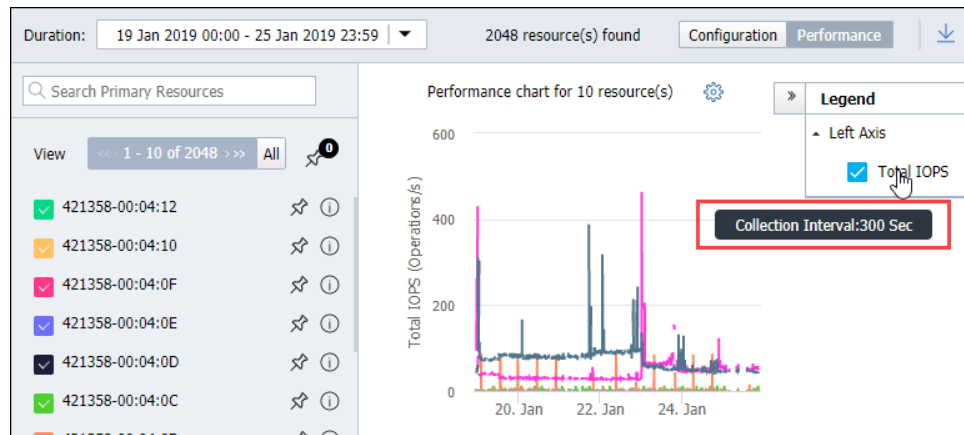
- f. Drag the **Filter** icon and select the **Total IOPS** filter.



- g. Click the  icon to exclude the Storage System resource, as displayed in the following screenshot:



- h. Click **View Result**.
- i. In the **View Result** window, hover over the metric name under **Legend**.
The current data collection interval of the metric is shown in seconds. For example, in the following screenshot, the collection interval is 300 seconds (5 minutes).



So, you can define the criteria for the Total IOPS metrics as follows:

- Correct:
 - 1 sample out of 5 minutes
 - 2 samples out of 10 minutes
 - 3 samples out of 25 minutes
 - 1 sample out of 10 minutes
- Incorrect:
 - 2 samples out of 5 minutes
 - 1 sample out of 1 minutes



Note: If you have set incorrect alert criteria, then delete the existing alert and add a new one. For deleting the existing alert, see [Managing alert definitions \(on page 78\)](#).

Identifying the metric value

Under certain circumstances, the Analyzer detail view cannot identify the value of the metric collected from the targets. You can find the actual value by running the query in Report Builder as described here.

Procedure

1. In the left pane, go to **Reports > Build**.
2. Click the **Create Using Query Builder** option.
3. In the **Create Using Query Builder** window, select resource group and resource.

After selecting the resource group and resource, the **Resource** and **Filter** options are enabled and a message to drag and drop the Filter or Resource is displayed.

4. Drag the filter and select the metric for which you want to identify the value.

5. Click **View Result**.
6. In the **View Result** window, click the **Configuration** tab.
7. Under the **Resource** column, click The value of selected metric is shown. For example: PSUS

15165-00:0C:02-15165-00:0C:10 Details		
Configuration	Related Resources	Configuration Changes
Resource Information		
Copy Type 1	Name 15165-00:0C:02-15165-00...	Primary Ldev DKC Model 8
Primary Ldev Number 00:0C:02	Secondary Ldev DKC Model 8	Secondary Storage Serial 15165
Status PSUS		

Managing detail view alert definitions

You can view an detail view alert definition, subscribe (or unsubscribe) to notifications, pause, or edit an alert.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the application bar area, click the **Alerts** menu, and select **Definitions**.
3. In the **Active Alerts** tab, click the **Filter** icon to filter alerts:

- Category
- Alert Name
- Severity
- Updated At
- Notification Status

4. In **Severity**, click the indicator to view the details.

The details section opens with the following links for managing alerts:

- **View Subscription Information:** You can view the notification information for a specific alert.
- **Subscribe or Unsubscribe:** To subscribe to email or Syslog, or SNMP notifications, select the email group, type the email, select the Syslog server information, or select the SNMP Manager, and then click **Subscribe**.



Note: SNMP Manager option is not available for System Alerts.

To unsubscribe, click **Unsubscribe**. (The default alert setting is **Unsubscribe**.)

- **Edit:** Refer to [Editing detail view alerts \(on page 79\)](#) for more information.
- **Pause:** You can pause the alert evaluation and the notification for a specific time period, and restart it later. The alert is moved to the **Paused Alerts** tab.
- **Delete:** You can permanently delete the alert definition.

Editing detail view alerts

You can edit the alert details such as threshold, target instances, alert conditions, and notifications. You can edit the alerts created through UI. Only the alert creator and the admin user can edit the alerts.



Note:

- Alerts added using the REST API cannot be edited using the UI.
- Alerts added using the UI in Analyzer detail view v10.5.0-01 or later cannot be edited using the REST API.
- For Analyzer detail view upgrades, alerts added using the UI in Analyzer detail view prior to v10.5.0-01 cannot be edited using the UI.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the application bar area, click the **Alerts** list and select **Definitions**.
3. In the **Active Alerts** tab, select an alert.
The details section opens.



Note: If the alert that you want to edit is paused, go to the **Paused Alerts** tab.

4. Click the **Edit** link.
The **Edit Alert** window is displayed.
5. In the **Alert Resource** section, you can edit the following details:
 - **Choose:** Select one or more target instances.
 - **Include future instances:** Automatically apply the alert to future target instances. (This option is only available if all target instances are selected.)
 - **For Instance(s):** Select the resource instance.



Note: The resource instances can be filtered based on certain criteria. For example, the disk type is displayed for `RAID Pool Tier` resource. You can filter the resource instances using the filter option (disk type) and then set alerts for the filtered resources. You can also choose to skip resource instances from the filtered list.

- **Include future instances:** Automatically include any future resource instances. (This option is only available if all resource instances are selected.)

6. In the **Alert Condition** section, you can set alert condition for the metric that was selected at the time of adding alert:

- For configuration metrics, provide the following details:
 - **Condition:** Select the condition type. Metrics with numeric values use: **greater than**, **between**, and **less than**. Metrics with string values use the **having** condition.

**Note:**

- Under certain circumstances, the Analyzer detail view cannot identify whether a metric is a numeric or string value. When this occurs, all condition types are listed in the GUI (greater than, between, less than, and having). To select the proper condition, you must know whether the metric is a numeric value or a string. You can find the value by running the query in **Report Builder**. See, [Identifying the metric value \(on page 77\)](#).
- If you are editing an alert with dynamic threshold, only the **greater than** and **less than** conditions are listed.

- **Threshold:** Depending on type of threshold (Static or Dynamic) defined when adding the alert, do the following:
 - **Static threshold:** Type or select a threshold value. (Certain metrics with string values include predefined thresholds.) The value set for the **having** condition is saved and is available for other users.

The threshold value specified in this field applies to all the selected resource instances.

**Note:**

- The threshold field supports alphanumeric characters, hyphen (-), underscore (_), comma (,), colon (:), at (@), slash (/), dot (.), and space.
- Switching between static and dynamic thresholds is not supported.

- **Customize Threshold For Resources:** Click this link to customize the value for a specific resource instance.

The **Customize Threshold for Resources** window is displayed. The instances selected in the **Alert Resource** section are displayed.

- Select the instances for which you want to customize the threshold. You can also filter the instances based on criteria, such as disk type.
- In the **Set Custom Threshold** field, enter a value and then click **Update**. The threshold value is updated for the selected instances.
- Click **OK**.

- **Dynamic threshold:** The dynamic threshold is derived by adding the values of Daily Moving Average (DMA) and Standard Deviation (SD). Analyzer detail view uses last 7 days data to calculate the DMA and SD values. Based on DMA and SD values, the dynamic threshold is determined everyday when a day is changed (as per Analyzer detail view application time zone). You can select one of the following options:

- 7 DMA + 1 SD
- 7 DMA + 2 SD
- 7 DMA + 3 SD

SD is calculated by applying a formula. 1 SD is a value derived from the formula. 2 SD and 3 SD is the value of 1 SD multiplied by 2 and 3, respectively.

Suppose, the DMA value is 20 and SD value is 10. The calculation will be as follows:

- 7 DMA + 1 SD = 30
- 7 DMA + 2 SD = 40
- 7 DMA + 3 SD = 50

**Note:**

- Dynamic threshold cannot be edited using REST API.
- Switching between static and dynamic thresholds is not supported.

- For a performance metric, enter the following details:
 - **Condition:** Select the condition type: **greater than**, **between**, and **less than**.
 - **Threshold:** Depending on type of threshold (Static or Dynamic) defined when adding the alert, do the following:

- **Static threshold:** Type the threshold value.

The threshold value specified in this field applies to all the selected resource instances.



Note: Switching between static and dynamic thresholds is not supported.

- **Customize Threshold For Resources:** Click this link to customize the value for a specific resource instance.

The **Customize Threshold for Resources** window is displayed. The instances selected in the **Alert Resource** section are displayed.

- Select the instances for which you want to customize the threshold. You can also filter the instances based on criteria, such as disk type.
- In the **Set Custom Threshold** field, enter a value and then click **Update**. The threshold value is updated for the selected instances.
- Click **OK**.

- **Dynamic threshold:** The dynamic threshold is derived by adding the values of Daily Moving Average (DMA) and Standard Deviation (SD). Analyzer detail view uses last 7 days data to calculate the DMA and SD values. Based on DMA and SD values, the dynamic threshold is determined everyday when a day is changed (as per Analyzer detail view application time zone). You can select one of the following options:

- 7 DMA + 1 SD
- 7 DMA + 2 SD
- 7 DMA + 3 SD

SD is calculated by applying a formula. 1 SD is a value derived from the formula. 2 SD and 3 SD is the value of 1 SD multiplied by 2 and 3, respectively.

Suppose, the DMA value is 20 and SD value is 10. The calculation will be as follows:

- 7 DMA + 1 SD = 30
- 7 DMA + 2 SD = 40
- 7 DMA + 3 SD = 50



Note:

- Dynamic threshold cannot be edited using REST API.
- Switching between static and dynamic thresholds is not supported.

- **Criteria:** Select the criteria. (The maximum value for minutes is 60.)

To select the proper alert criteria you must know the data collection interval of the metric, see [Identifying the collection interval \(on page 73\)](#).



Note: If you want to add alerts for the metrics with a data collection interval exceeding 60 minutes, you must configure the data collection interval for these metrics up to 60 minutes on the RAID Agent.

- **Monitor Between:** Select the monitoring time. Alert monitoring window is based on UTC timezone. Be sure to select the appropriate time window. If applicable, also consider the Daylight Saving Time. For example, if the Analyzer detail view UI timezone is set to Pacific Time (GMT-08:00) and you want to add alert for time window 9:00 AM to 7:00 PM, then set alert monitoring window as 05:00 PM to 03:00 AM.

7. In the **Alert Notification** section, click the **Email**, **Syslog**, or **SNMP** tab and provide the following details:

- **Email:** Select the email groups to which you want to send the notification, or type the individual email address. You can choose any of the following options:
 - **Each alert violation:** Sends a notification on every alert.
 - **Hourly or Daily:** Sends notification hourly or daily.
 - **The first alert violation:** Sends the first violation alert and suppresses subsequent alert notifications when alert violations happen for an extended period. Sends the second notification when the alert condition is ended.



Note: You can add email groups in **Manage > Manage Email groups** and the email address in **Manage > Manage SMTP**.

- **Syslog server:** Select the Syslog server.



Note: You can configure the Syslog server in **Manage > Manage Syslog**.

- **SNMP Manager:** Select the SNMP Manager.



Note:

- You can configure the SNMP Manager in **Manage > Manage SNMP**.
- If you select SNMP Manager, alert violations on the real-time data are not sent to the SNMP Manager.

8. Click **Update**.

Viewing detail view alert summaries

The Alert Summary tab shows a high-level summary of the alerts generated globally.

The Alert Summary tab is always visible by default when you open the detail view GUI and expand the nodes in the resource tree. If you close the tab, you can always reopen it.

In the application bar area, click the **Alerts** menu, and select **Summary**.

Viewing detail view alert violations

You can view the details of alert violations based on the resource for which the alert occurred.

Procedure

1. Select **Tools > Ops Center Analyzer detail view** to start the detail view GUI.
2. In the application bar area, click the **Alerts** menu, and select **Violations**.
The **Alert Violations** tab opens.
3. Click the plus icon (+) to view details and a graph of the violation.
4. In the **Acknowledge** column, select the check box to acknowledge the alert if you created it.



Note: The alerts generated on the real-time data will start showing under the **Alerts Violation** tab, only after the data (for which the alert is generated) is collected through default flow.

Chapter 5: Working with Analyzer detail view reports

You can add your own reports for a resource in the resource tree or in the Reports dock.

Adding user-defined reports in the resource tree

Analyzer detail view provides a set of default reports on the resource tree nodes. These reports help you to manage resources in your environment (storage systems, switches, hosts, and hypervisors). However, you might need to add your own reports in the following scenarios:

- **To suit your infrastructure requirements:** Analyzer detail view provides you the flexibility to create your own reports so that you can choose metrics that best suit your infrastructure.
- **To monitor metrics for which default reports are not available:** While every probe collects a set of metrics, some metrics are optionally collected using certain collection methods. Default reports are not provided for these metrics, but you can add the reports for these metrics.

For example, the **Total Response Time** metric of **RAID Port** resource is collected by Hitachi Enterprise Storage probe (when the RAID Agent storage system instance is added using the SVP method). You can add a report for this metric using this procedure.

Refer to *Hitachi Analyzer Detail View Metrics Reference Guide* for data collection methods.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. You can add a new report in two ways:
 - In the resource tree, right-click the node in which you want to add a report, and then click **Add Report**.

For example, click on **Hitachi > VSP G/VSP F/VSP E > Storage-system-instance-node > Ports** node and then click **Add Report**.
 - In the Reports dock, click **+ Report**.

For example, click on **Hitachi > VSP G/VSP F/VSP E > Storage-system-instance-node > Ports** node and then in the **Reports Dock**, click **+ Report**.

The **Add Report** window opens.
3. In the **Report Name** field, type the report name.

4. Click **Add Metrics**.

The window displays a list of related resources and metrics.

For example, select the **Ports** resource from the **Resource(s)** list and then select the **Total Response Time** metric from the **Select metric(s)** list.



Note: You can add a maximum of 15 metrics (total in left and right axis).

5. Click **Add**, and then click **Save**.

The report is added in the reports pane for the selected node in the resource tree and Reports dock.

Working with the Reports dock

You can access reports by clicking a report template in the Reports dock. The Reports dock is located at the bottom of the Reports pane, and displays the report templates for the selected Resource tree node.

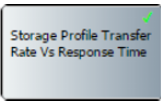
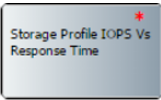
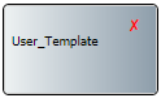
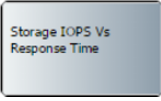
Adding new reports in the detail view Reports dock

You can build your own new custom performance report templates in the Reports dock. In the Reports dock, click **+ Report**.

For details, refer to [Adding user-defined reports in the resource tree \(on page 86\)](#)

Adding existing reports from the detail view Reports dock

You can add an existing report from the Reports dock to the Reports pane. The following icons indicate the status of reports in the detail view Reports dock.

Icon	Description
	The report has been added to the Reports pane.
	The report has been added to the Reports pane but not saved. After you save the report, the icon changes to a green check mark.
	You can delete reports you added. (You cannot delete default reports.)
	The report has not been added to the Reports pane.

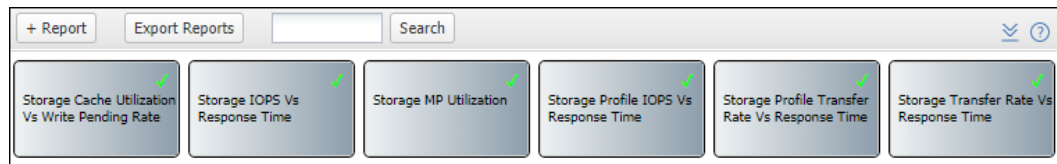
Procedure

1. Click the report you want to add.
The report is displayed in the **Reports** pane, and the report status becomes a red asterisk.
2. Click **Save**.
The report is saved, and the report status becomes a green check mark.

Searching detail view report templates

You can search for a specific report template from the detail view Reports dock.

Specify the criteria and click **Search**.



For example, if you type IOPS, report templates that include "IOPS" are displayed.

Exporting detail view reports in batch

You can export all the reports for a selected tree node.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the Reports dock, click **Export Reports** to start the export of all the reports. (**Export Reports** is enabled after all reports in the tab are loaded.)

The export function is only available for the Configuration and Performance views.

It might take time for all the reports to be exported and ready for download. The reports are exported in a compressed file. The file name contains the node and tab information for easy reference (for example, VSP_VSP53004_configuration.zip).

Result

Chart reports are exported in PDF format with the following names:

Chart_Reports_xxx_performance.pdf

Chart_Reports_xxx_configuration.pdf

where xxx is the node identifier (for example,

Chart_Reports_VSP_VSP53004_performance). The data for the chart reports is exported to an Excel file with the .xls extension. The data for each chart is saved in a separate worksheet.

General considerations

- Some reports contain charts and tables (such as Capacity Reports on the Storage Systems). The chart reports are exported to PDF, and table reports are exported to Excel files.
- A maximum of top 20 resources are exported. However, if the report has user-defined Top-N (number or percent), then it takes precedence over the global TopN-for-export property.
- Charts do not consider any UI feature such as Zoom , Compare With, and changed unit of measure (reports are exported in the default view).
- Any filters applied to tables are ignored (all the data is exported).
- If data is not available, exported charts or tables contain the following message:

`No data available`

Chapter 6: Using Analyzer detail view reports

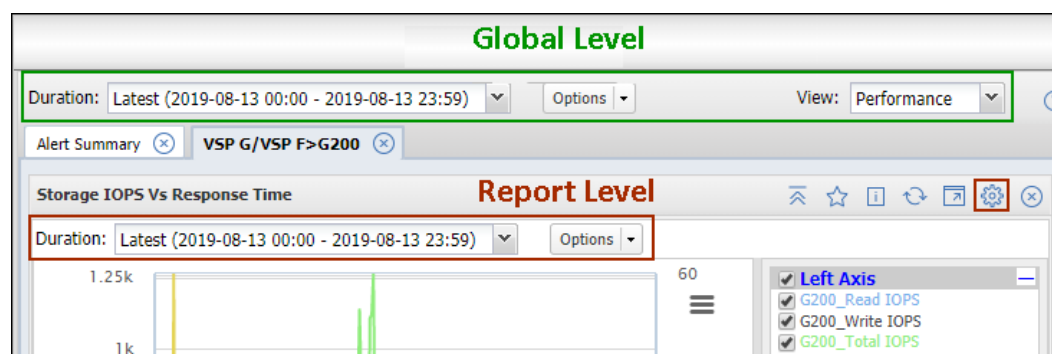
You can access reports by selecting a resource in the Resource tree or clicking a report template in the Reports dock.

Managing Analyzer detail view report settings

Analyzer detail view has predefined default settings for the reports. However, you can customize the reports to meet your requirements.

You can modify report settings at two levels:

- **Global:** Changes applied at this level are reflected in all reports.
- **Report:** Applies only to the current report. To display the report options, click  in the Report window.



Each setting has a global and report-level counterpart, with the following exceptions that only apply at the global level:

- **Options:**
 - **Settings:**
 - **Schedule:** The running frequency of the report.
 - **Use Near Real Time:** The default view of the report in near real time.
 - **Top N Chart:** The number of Top N resources to view in the report.
 - **On Zoom:**
 - **Sync Reports:** If any of the reports on the active tab are in zoom-in view, use this option to zoom in to all the other reports. After you select this option, all the other reports are synced with the zoomed report.
 - **Recalculate Top N:** If any of the reports on the active tab are in zoom-in view, use this option to recalculate the resource option using the zoomed window. The resource order changes based on the zoomed window, with the most used resource at the top.

Changing report scheduling (detail view global options in reports pane)

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the **Reports** pane, click the **Options** menu.
3. Click **Settings** from the available options.
By default, all the chart reports run daily. However, reports can also be run weekly and hourly.
4. In the **Schedule** section, select the frequency:
 - **Hourly**
 - **Starting at Minute of hour:** Select the starting time (minutes) for report generation. For example, select 15 (minutes).
 - **Duration (Hours):** Select the number of hours for which the report must generate. For example, select 4 (hours).
 - **Daily**
 - **Starting at Hour of day:** Select the starting time (hour) for report generation. For example, select 17 to indicate 5 PM.
 - **Duration (Hours):** Select the duration in hours for which the report must run. For example, select 4 (hours).
 - **Weekly**
 - **Starting at day of week:** Select the starting day for report generation. For example, select **Mon**.
 - **Duration (Days):** Select the duration of weekdays. For example, select 1. The system considers value 1 as Tuesday, value 2 for Wednesday, and so on.

5. If you want to view the reports with the latest data, select the **Use near-real-time data** check box.
6. For the **Top-N chart**, perform the following:
 - a. Define how many charts to plot. Select the number from the **Chart for Top** list.
 - b. Select **# Left axis resources** or **% Left axis resources**. For example, if you select **# Left axis resources**, the chart report shows the top 10 resources of the total resources. If you select **% Left axis resources**, the chart report shows the top 10 percent of the total resources.
7. Click **Save**.

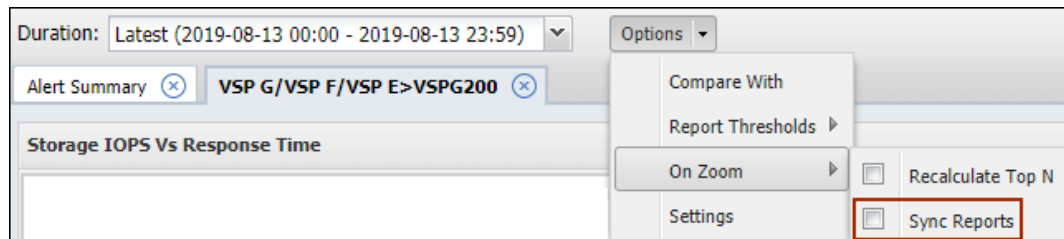
Using On Zoom (detail view global options)

The On Zoom option provides the Recalculate Top N and Sync Reports features. To apply these features to detail view reports, zoom in to the report on the active tab.

With the zoom-in feature you can expand any portion of a chart to view the details of the data points.

Procedure

1. In the **Reports** pane, select the report area that you want to view by clicking and dragging the cursor.
The report zooms in.
2. To zoom out, click reset zoom  (in the lower-left corner) of the report.
3. You can apply On Zoom to other reports with the Sync Reports feature. In the **Options** menu, select **On Zoom > Sync Reports**. All the other reports are then synced with the zoomed report.



4. Recalculate the resources with the **Recalculate Top N** feature. After you select this option, the resource order changes based on the zoomed window, and the most used resource during that time period is at the top.
5. To recalculate the resources, in the **Options** menu, select **On Zoom > Recalculate Top N**.

Changing the detail view report duration

You can view the historical report using the Custom Duration option in the Duration menu.



Note: In the Global options, you can rename an entry in the Duration menu by clicking the pencil icon. The named entries are then displayed under Saved Durations in the menu.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the **Reports** pane, click the **Duration** menu, and select **Custom Duration**.
3. Specify the duration for which you want to view a report (maximum: 7 days) and click **OK**.

Hitachi Enterprise Storage performance reports support a duration of one year. If you select the duration longer than 7 days, the data is rolled up and the data granularity of a report is plotted on a pre-defined structure as the following:

Duration	Data granularity
8 days to 1 month	2 hours
1 month to 3 months	4 hours
3 months to 6 months	8 hours
6 months to 12 months	24 hours

You can view the data rolled-up status on the **Status** window. For more information refer to, [Viewing data processing status \(on page 115\)](#).



Note: Regardless of the duration that you select, the data granularity also depends on the resource availability. For example. If you select 12 months and the resource that you are viewing is available only for 6 months, the data is rolled-up based on a pre-defined structure of 6 months duration and the data granularity is 8 hours.



Note: A probe ID is used internally to identify a probe. Suppose you have added a probe in the past for a target. Over a period, you deleted the probe and re-added a new probe for the same target. Due to some reasons, the probe IDs for the old and newly added probe are different (even if the target is the same). In that case, you can only select the duration for which the newly added probe has collected data under the Resource tree subnodes in the Analyzer detail view UI.

For example, suppose you have added the Hitachi NAS probe for a storage system with a "4001" serial number, and its data is visible on the Analyzer detail view UI from June-01 to June-14. Over a period, you delete the Hitachi NAS probe and add the Hitachi NAS (REST API) probe for the same target, and its data is visible on the Analyzer detail view UI from June-15 to June-30. Due to some reasons, the probe IDs for the old and newly added probe are different. In such a scenario, under Resources > Storage Systems > HNAS > *HNAS-System-Name* > Storage Pools > *Storage-Pool-Instance* subnode, you can select the report duration for only the newly added probe (June-15 to June-30).

If you want to view reports on the *Storage-Pool-Instance* subnode for any duration between June-01 to June-14, click the *HNAS-System-Name* node, select the required duration, and then select the *Storage-Pool-Instance* subnode. The reports are displayed for the selected duration in the Reports pane.

Changing the detail view report date

You can change the report date to display data from a specific date.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the **Reports** pane, click the **Duration** menu, and select **Change Date**.
3. Select the date for which you want to view a report.
4. Click **OK**.
The report for that period is displayed.

Comparing detail view report intervals

You can compare the current resource assessment either with the last report run or with a historical report run.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. To compare with the historical report run (not the last report run), first select the duration from the **Duration** menu.
3. In the **Reports** pane, from the **Options** menu, select **Compare With**.
4. Specify the historical time period for which you want to compare the assessment.
The comparison displays with different colors and dotted lines in the report.

Changing the view of a report

You can change the view of a report by isolating a graph, changing the metrics or thresholds used, altering the plot method, or changing the unit of measure.

Isolating resources in a chart report

You can isolate resources for viewing in the chart report.

Procedure

1. In the report area, click the **Options** menu.
2. Click **Settings**.
3. In the **Resources** section, select the resources that you want to display in the chart report.

The reports for only the selected resources are displayed.



Note: If the assessment of more than one resource is plotted in a chart report, you can view each resource separately.

4. Restrict the resources to display by choosing the required number from the **Limit number of Resources** displayed per page list.

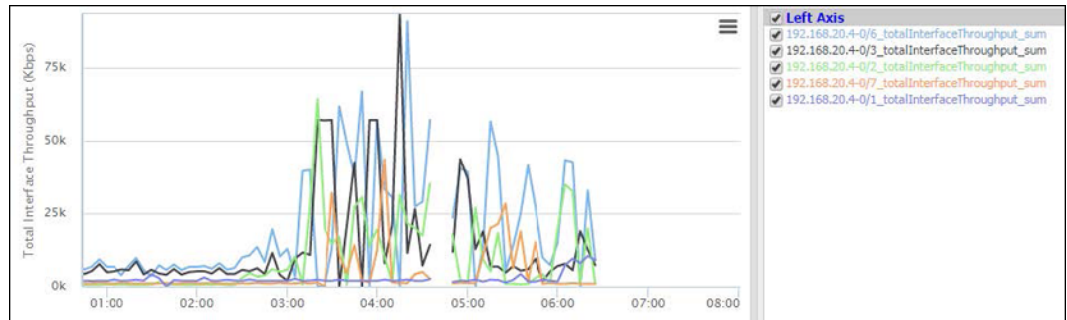


Note: Maximum 50 resources can be displayed per page in a chart report.

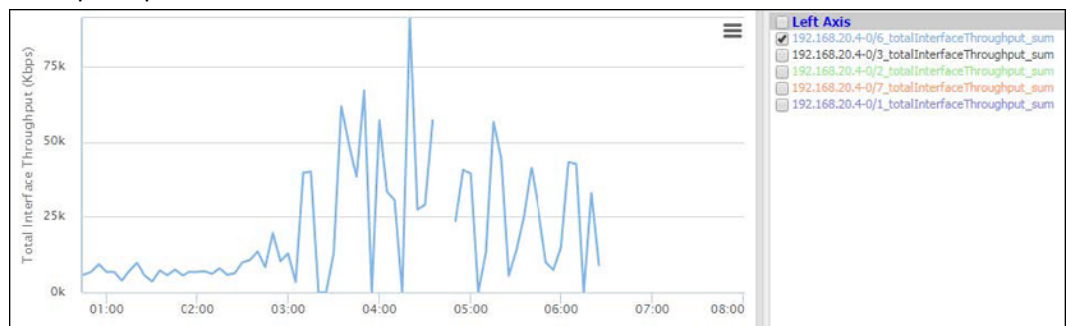
5. Click **Update**.
The report opens with the selected resources.
6. On the upper-right corner of the report, click **Save**.
You can also select or deselect resources directly on the chart. By default, every chart report shows an assessment for one or more resources. If the assessment of more than one resource is plotted in a chart report, you can view each resource separately. To do

so, you need to cancel other resources. The following screen shots show the differences.

- Example report with all resources selected.



- Example report with one resource selected.



Isolating metrics on a chart report

You can select the metrics for viewing in the left and right axis.

Procedure

1. In the report area, click the **Options** menu.
2. Click **Settings**.
3. In the **View Settings** section, select the metrics to view in the left and right axis.
The selected metrics are displayed in the report.
4. Click **Update**.
The report is displayed in the **Reports** pane.
5. In the upper-right corner of the report, click **Save**.

Changing the plot method of a chart report

You can change the plot method used to display the data.

Procedure

1. In the report area, click the **Options** menu.
2. Click **Settings**.

3. In the **View Settings** section under **Display**, select one of the following options:
 - Area
 - Line
 - Line (Interpolate)
 - Scatter
 - Stack
4. Click **Update**.
5. In the upper-right corner of the report, click **Save**.

Changing the threshold of a chart report

The Threshold Setting option allows you to alter the threshold on the chart report. You can choose the predefined thresholds or add a new threshold.

You can also add a new threshold from the Manage Threshold window. For more information, refer to [Customizing detail view dashboard indicator thresholds \(on page 63\)](#).

Procedure

1. In the report pane, click the **Show report setting** () icon.
2. In the report area, click the **Options** menu and then select **Settings**.
3. In the **Thresholds Settings** section, select the **Enable Thresholds** check box.
4. Select a threshold value from the **Threshold** column.
5. To set the new threshold value, from the **Threshold** column, select **Add threshold**. The **Add Threshold** window opens.
6. Enter the following details and click **Save**:
 - a. Type the threshold name and set the threshold value.
 - b. Configure **Advanced options** to set threshold direction (Forward or Reverse):
 - For **Forward Threshold**, the critical threshold should be greater than warning threshold. In this case, the threshold is violated when the metric value exceeds the defined threshold. By default, the threshold direction is **Forward**.
 - For **Reverse Threshold**, the warning threshold should be greater than critical threshold. In this case, the threshold is violated when the metric value is less than the defined threshold. Reverse direction thresholds are useful when evaluating metrics like Read Hit for VMAX Volume or Cache Usage. If the Read Hit rate falls below the threshold, the cache is underutilized and performance suffers.
7. Click **Update**.

Changing the unit of measure for chart reports

The option to change the unit of measure provides you the flexibility to change the unit of measure to understand report more easily. You can change the unit of measure for reports that displays the unit (bytes, bytes/s, KB, KB/s, MB, MB/s, GB, GB/s, and TB, TB/s). After

changing the unit of measure, the changes are saved automatically in the system and are visible to other users.

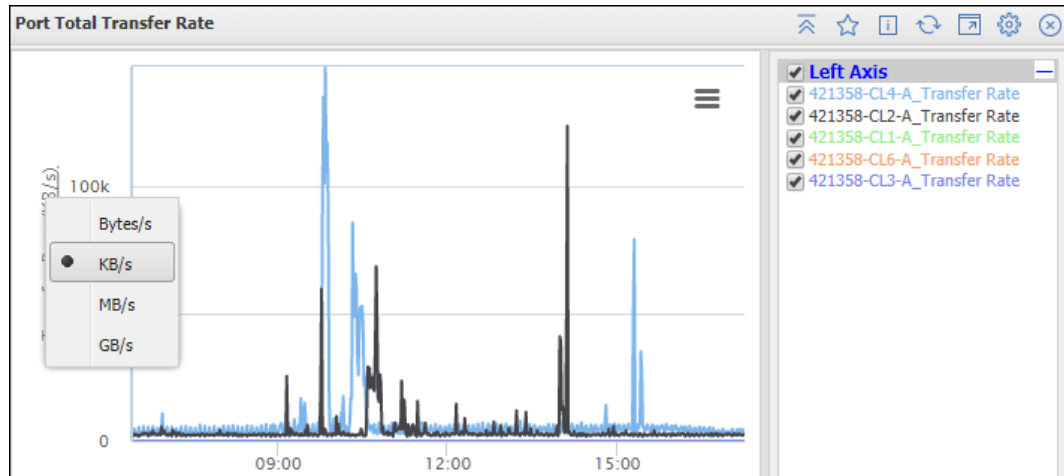


Note: Changing the unit of measure of a report only changes the display of the report. It does not change the value of the metric in the database.

Procedure

1. In the report area, click on the unit of measure option next to the left or right axis label. The available options are shown.

Example of the report with unit of measure option.



2. Select the unit of measure, in which you want to view the report. Report downloads will also display the selected unit of measure.



Note:

- While adding the custom report, if you add more than one resource to the left or right axis, then you cannot change the unit of measure.
- For Internet Explorer users: If a problem occurs while changing the unit of measure of a report, then you must verify that the Scripting option is enabled in the Internet Explorer settings. To do so, go to Settings > Internet Options > Security > Internet > Custom Level > Scripting, enable all setting under the Scripting option. Close the Internet Explorer browser and restart your computer.

Viewing the query for an existing report

The Show Query option allows you to view the MQL query associated with the report.

Procedure

1. In an open report, select **Options > Show Query**
2. The MQL query is displayed in a box. You can cut and paste the text and modify it for use in a custom report or with the Analyzer detail view REST API.

Downloading and printing detail view reports

You can download chart reports as an image (PNG, JPEG, or SVG vector), a PDF document, or CSV data.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the report area, click .
3. From the shortcut menu, choose from the following options:
 - Download PNG image
 - Download JPEG image
 - Download SVG vector image
 - Download PDF document
 - Download CSV data

Report downloads show only the current visible resources on the chart report.

Adding detail view reports to Favorites

The **Favorites** node contains shortcuts to all reports you have added as favorites.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the report area, click the star icon.
The **Add a report as favorite** window opens.
3. In the **Save As** field, customize the report name if you want.
4. Click **Done**.
5. To view your favorite reports, click the **Favorites** node in the Resource tree view.
The node opens with all reports that you saved.
6. To remove a report from your favorites, click the **X** icon and confirm your choice.

Understanding the owner name used by the Analyzer detail view

On the Analyzer detail view, the owner represents the hosts where LDEVs are mapped to the host group. When a group of LDEVs that are using a common set of WWNs are mapped to multiple host groups, then the owner name is created by combining the name of these host groups. Therefore, an owner is not the same as the host group.

The Analyzer detail view creates the owner only for the Hitachi Enterprise Storage probe by applying the following rules:

Rule 1: The unique name is discovered from the list of host groups and sorted in case-insensitive alphabetical order.

Rule 2: Length of the common string is checked. If the common string is the name of the host group, then the last character is skipped from the common string.

Rule 3: If the common string of the host group is less than three characters, then the owner name consists of the host groups separated by an underscore (_).

Rule 4: If the common string of the host group name is three characters or greater, then the owner name consists of the common sub-string appended by a hyphen (-) and the remaining part of the host group name is separated by an underscore (_).

Rule 5: If the resulting owner name is greater than 50 characters, it is truncated as follows.

- a. If the owner name has a hyphen, the name is truncated at the hyphen.
- b. If the owner name does not have the hyphen (-), then the first 50 characters become the owner name.

Rule 6: If non-unique owner names are obtained after applying the rules, then the owner name is appended with (0), (1), and so on.

The owner name depends on the configuration data collection. If there is any change in the components that are used to create the owner name, the owner name is changed after the latest configuration data is collected.

Example 1:

The group of LDEVs 00:01:01 and 00:01:02 having a common set of WWNs are mapped to the following host groups:

```
ESXI_COMTest
DC1_ESXI_COMTest_NEW
DC1_ESXI_COMTest_NEW_M4
ESXI_COMTest
COMP_test
```

1. After applying rule 1 on the above host groups, the following output is created:

```
COMP_test
DC1_ESXI_COMTest_NEW
DC1_ESXI_COMTest_NEW_M4
ESXI_COMTest
```

2. According to rule 2, the common string is searched and starts matching with the first character. Because there is no common string in these host groups name, the length of the common string is considered zero (0) and rule 3 is applied so that the owner name contains all the host group names separated by an underscore (_) and the owner name becomes:

```
COMP_test_DC1_ESXI_COMTest_NEW_DC1_ESXI_COMTest_NEW_M4_ESXI_COMTest
```

3. As the length of this owner name exceeds 50 characters and it does not have a hyphen, the length restriction rule 5b applies and the following owner name is created:

```
COMP_test_DC1_ESXI_COMTest_NEW_DC1_ESXI_COMTest_NE
```

Example 2:

The group of LDEVs 00:01:03 and 00:01:04 are mapped to following host groups:

```
COMP_test
COMP_test22
```

1. After applying rule 1, the following output is created:

```
COMP_test
COMP_test22
```

2. The common string is `COMP_test`. According to rule 2, if the common string is the name of the host group, then the last character is skipped:

```
COMP_tes
```

3. The length of the common string is eight characters in this case (greater than three characters). Therefore, rule 4 is applied and the owner name contains the common substring appended by a hyphen and the remaining part of the host group name is separated by an underscore. The resulting owner name is: (rule 5 does not apply because the name is less than 50 characters.)

```
COMP_tes-t_t22
```

Renaming instance-level nodes in the resource tree

You can change the instance-level node names in the resource tree. The new name is reflected in the following features:

- Resource tree view reports
- Alerts feature
- Health Check (table reports, performance chart reports, and real-time reports)
- Workload Analysis report (table reports and performance chart reports in UI, and in the downloaded PDF reports)
- Reports generated in Reports Scheduler:
 - Health Check
 - Inventory
 - Replication
 - VSM Summary
 - Workload Analysis

Procedure

1. In the resource tree, right-click the instance-level node that you want to rename, and then click **Rename**.
2. Enter the new name, and then press **Enter**.
3. Click **Yes** to confirm.



Note: If you want to restore the system-defined (default) name, you can revert it with the **Undo Rename** (↶) option which is displayed when you hover over the renamed node in the resource tree.

Creating custom reports using the Analyzer detail view Report Builder

The Ops Center Analyzer detail view Report Builder enables you to create your own queries and generate reports. The Report Builder provides a comprehensive, extensible and reusable reporting infrastructure that is based on a regex-based query language (MQL) that retrieves and filters the data in the Analyzer detail view database. MQL allows complex analysis in real time with constant run-time. MQL syntax makes it possible to traverse relations, identify patterns in the data, and establish a correlation.

Using Report Builder, you can create a report of resources and associated metrics that you want to monitor closely. You can also extend the Analyzer detail view built-in reports.

The first step is determining the resource and metrics that you want to analyze. You can identify this by using the UI reports or the one you want to monitor closely, and then create the custom report using one of the following methods:

- Build a query using the UI: Use the **Create Using Query Builder** option to build a query for creating a report.
- Write a query: Use the **Create Using MQL** option to write a query for creating a report.

To access the Report Builder, go to the Analyzer detail view UI and from the left pane, click **Reports > Build**.

Creating a report using Query Builder

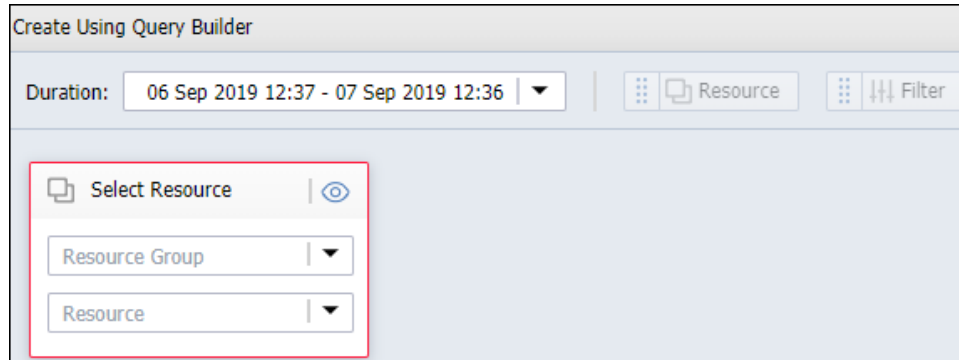
The Query Builder helps you generate reports with a simple UI. It allows you to select the resource and apply filters. For example, you can run a simple query that shows the list of LDEVs across the same resource (such as, Hitachi Enterprise storage system).

The query is built on the following:

- **Resource group:** Resource groups are the types of targets that are monitored using the Analyzer probe. For example, if you want to troubleshoot an Hitachi Enterprise storage system, you must select the Hitachi Enterprise Storage resource group.
- **Resource:** There can be multiple resources associated with a resource group. For example, the pool, LDEV, and MPB are resources associated with Hitachi Enterprise Storage resource group.
- **Filter:** Use the filter to select the metrics associated with a resource. For example, if you select the Pool resource, the pool ID and total IOPS are available as filters. In a query, you can add multiple filters for a resource.

Procedure

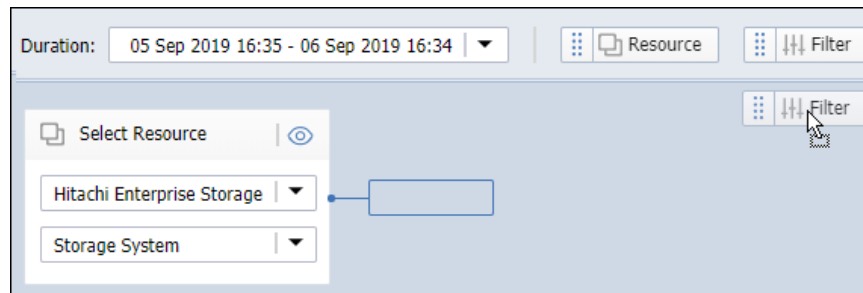
1. In the Analyzer detail view left pane, select **Reports > Build**.
The **Build** window opens.
2. Click **Create Using Query Builder**.
3. In the **Create Using Query Builder** window, use the **Select Resource** box to start building a query.



4. Let's assume you want to build a query that shows the total IOPS of the LDEVs associated with Hitachi Enterprise Storage system serial number 421358.
 - a. Select the **Resource Group** and **Resource** that you want to query.

In this example, we will select the **Hitachi Enterprise Storage** resource group and the **Storage System** resource.

After selecting the resource group and resource, the **Resource** and **Filter** options are enabled and a message to drag and drop the Filter or Resource is displayed.
 - b. To add the filter, drag the **Filter** icon as follows:

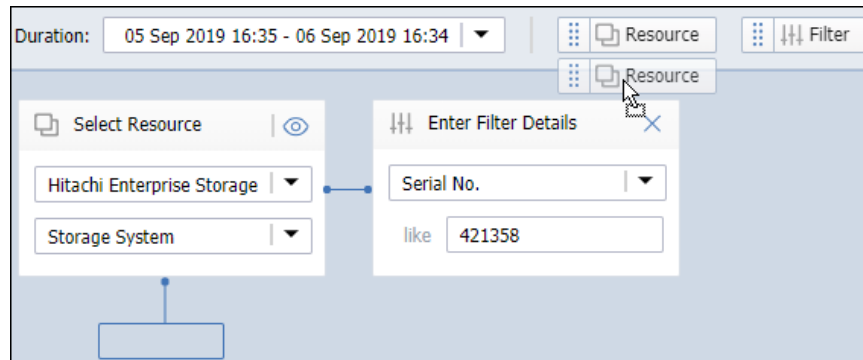


The **Enter Filter Details** box is added next to the **Select Resource** box.

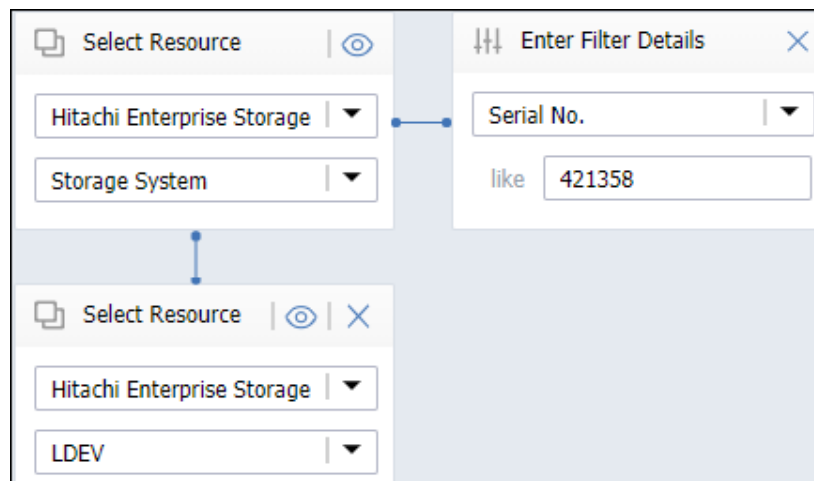
- c. Select the **Filter**. Metrics corresponding to resource are listed. After you select the metric, you have the option of drilling down your query by applying filters:
 - If a configuration metric is selected, you can enter a string in the **like** box. You can also enter a regular expression.
 - If a performance metric is selected, you can apply the conditions like (Any, between, less than, or more than) for (at least, at most, or exactly) samples.

To query storage system serial number 421358, we will select the **Serial No.** metric and then enter 421358 in the **like** box.

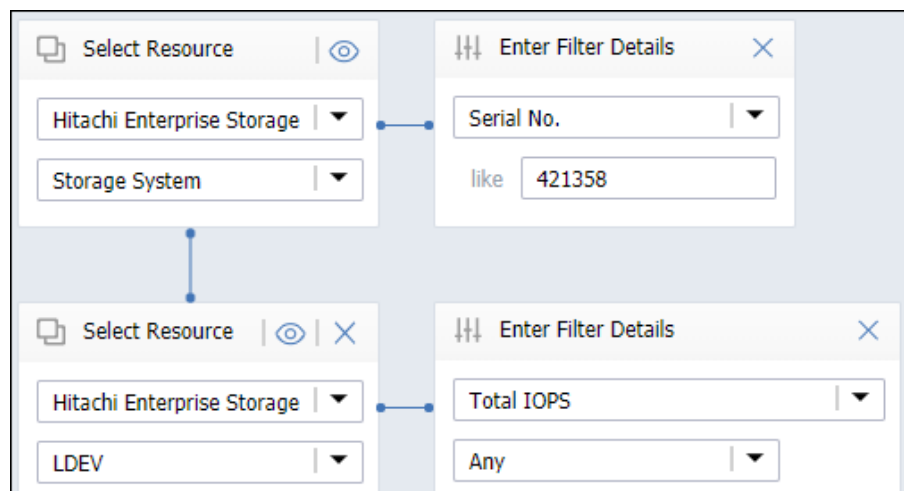
- d. To query the total IOPS of LDEVs, you must add the LDEV resource. Drag the **Resource** icon as follows:



- e. Select the **Hitachi Enterprise Storage** resource group and **LDEV** resource.

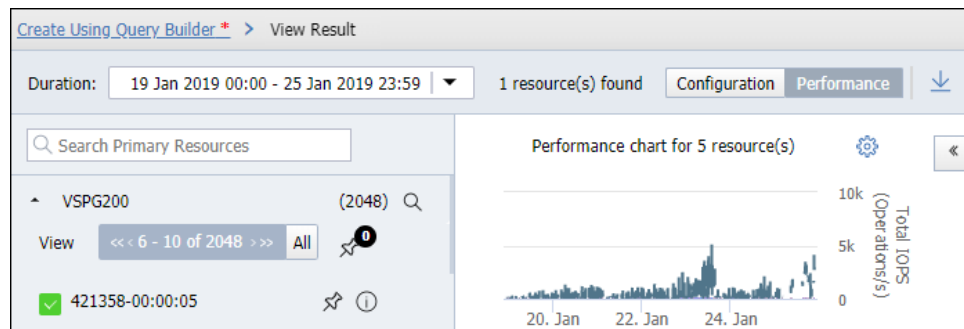


- f. Drag the **Filter** icon and select the **Total IOPS** filter (apply other filters as required). For creating the sample report, make sure that you have created the query as shown in the following example.



- g. In **Duration**, select the length of time to run the query (maximum 7 days).
h. Click **View Result**.

The **View Result** window opens. See [Viewing reports in Report Builder \(on page 107\)](#) for more details.



**Note:**

- An asterisk (*) in the breadcrumb indicates that the query is not yet saved. If you want to make any changes, you can use the breadcrumb to return to **Create Using Query Builder** window.
- You can drill down by applying multiple filters for resources as shown in the following example.

- You can add multiple resources as shown below. A maximum of two resources can be viewed in the report. For example, if three resources are added in a query, then the top 1 resource will be excluded in the report. In the following example, the Storage System resource is excluded and not be shown in the report.

If you delete any resource from the query, the resource will be enabled in reverse order.

- You can exclude resources from the report using the icon in the **Select Resource** box.

5. In the **View Result** window, click **Save Query** and enter the query name.
6. Click **Save**. The query is saved and listed in the **Build** window.

Creating a Analyzer detail view report using MQL

MQL is intended for more complex operations than the Query Builder. This includes operations such as interval rollup and resource rollup. Refer to the *Hitachi Ops Center Analyzer Detail View Query Language User Guide* for details. You can write a query from the scratch or you can extend the queries of built-in reports.

Procedure

1. In the Analyzer detail view left pane, select **Reports > Build**.
The **Build** window opens.
2. Click **Create Using MQL**.
3. Enter a query in the **Enter MQL** box:
 - **Writing queries from the scratch:** For example, the following query uses the interval rollup operation to aggregate data from a lower interval to a higher interval:

```
raidPG[@utilization rx b .*]{intervalRollUpOp=AVG,outputIntervalInSec=3600}
```

By default, the collection interval of utilization metric of the RAID PG group is 300 seconds. This example query uses 3600 seconds (`outputIntervalInSec`) query filter option.

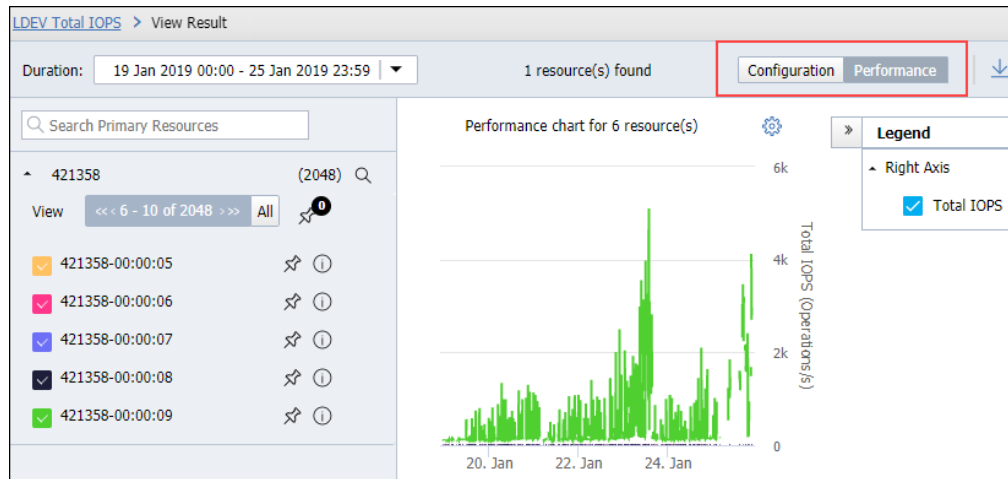
- **Extending queries of built-in performance reports:** To extend queries of existing reports, do the following:
 - a. Go to resource tree node.
 - b. In a chart report area, click the  icon and select **Options > Show Query** and then copy the query.
 - c. Go back to **Reports > Build**.
 - d. Paste the query in the **Enter MQL** box.
 - e. Edit the query as required.
4. In the **Duration** box, select the length of time to run the query (maximum 7 days).
 5. Click **View Result**.
The **View Result** window opens.
 6. In the **View Result** window, click **Save Query** and enter a name.
 7. Click **Save**. The query is saved and listed in the **Build** window.

Viewing reports in Report Builder

Based on the query, Report Builder generates configuration and performance reports. If a query contains performance metrics, both performance and configuration reports are generated. If a query contains only configuration metrics, only the configuration report is generated.

At the top of the **View Result** window, you can choose to view the configuration and performance report. You can also change the report duration.

Viewing a performance report



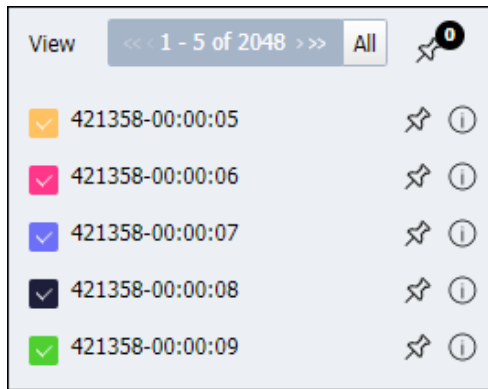
Item	Description
	List of primary and related resources: A primary resource is the first resource in your query. If you have queried the LDEV IOPS for a storage system, the storage system is the primary resource and the LDEV is related resource. In this example, 421358 (storage system) is primary resource and 421358 - 00:00:05 (LDEV) is secondary resource. Under View, five related resources are listed. You can view other related resources using the or icons.
	Chart report: By default, the primary resource metric is displayed on the left axis and the related resource metric is displayed on the right. If a query contains only one resource, a default of ten primary resources are displayed. If a query contains two resources with filters on both resources, 6 resources (1 primary and 5 related resources) are displayed.
and	See Pinning a resource in chart report (on page 109) for more information.
	Chart settings: By default, all the chart reports are plotted in line (plot type) with linear scale. When you

Item	Description
	click this icon, the Chart Settings window is displayed. You can define the following chart settings: - Left and right axis scale: - Linear - Logarithmic - Left and right axis plot type: - Area - Line - Line interpolate - Scatter - Stack - Metrics on left and right axis
	Indicates that the performance data is not available for the resource.
	Use this icon to view the details of an individual resource: - Configuration - Related resources - Configuration changes - Relation changes
	Hide or show the chart legends.
	You can choose to hide the metrics on chart. Also, when you hover over the metric name, the data collection interval for the metric is displayed.

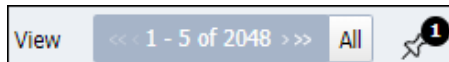
Pinning a resource in chart report

The pin  icon allows you to create a group of resources that you want to view in one chart report. You can compare the pinned resource with other resources across all the pages.

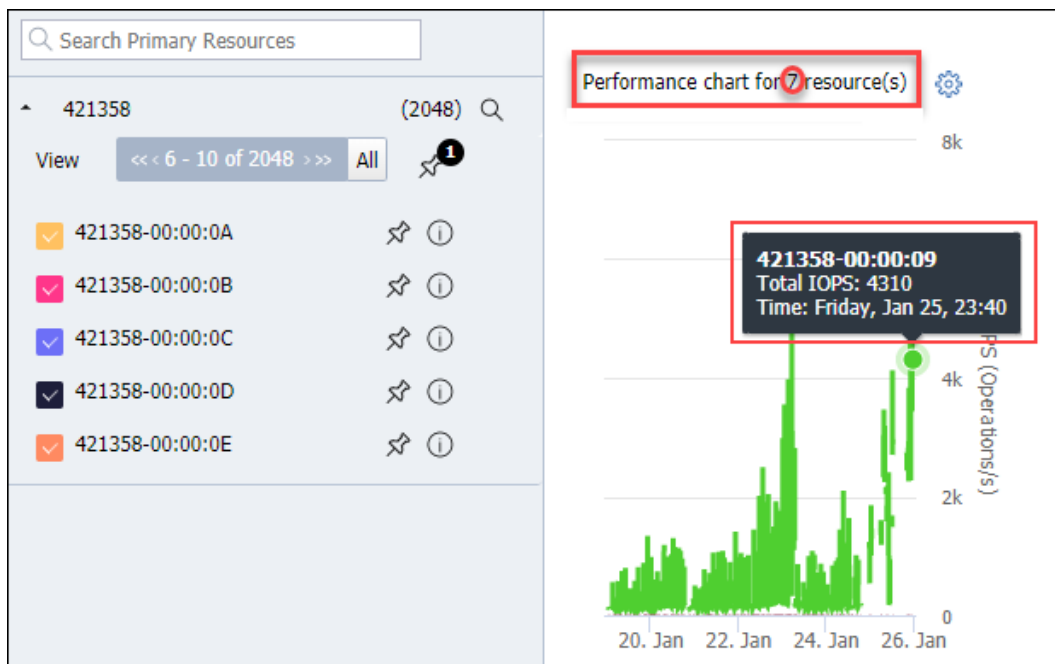
As shown in the following example, resources 1-5 are listed. If you want to compare the **421358-00:00:09** resource with other resources (for example 6-10) on other pages, you must pin this resource.



When you pin a resource, the number of pinned resources is shown as follows:



When you view another set of resources, the performance chart of the pinned resource is plotted. In the following example, the pinned resource (421358-00:00:09) is displayed along with resources 6-10. Also, the number of resources is increased to 7 in the chart report (5 related resources + 1 pinned resource + 1 primary resource).



Viewing a configuration report

Click the **Configuration** tab to view the configuration report for a resource.

[LDEV Total IOPS](#) > View Result

Duration: 19 Jan 2019 00:00 - 25 Jan 2019 23:59 | 1 resource(s) found | Configuration | Performance

Resource	Model Name	Name	Serial No.	Vendor Name
VSPG200 ⓘ	VSP G200	VSPG200	421358	HITACHI

In this example:

- The configuration report is displayed for resource VSPG200 along with its serial number 421358 and other details such as name and model name. This is the primary resource. If you want to see more details, click ⓘ.
- To view related resources, click the resource (VSPG200 in this example). The list of all related resources is displayed.

Exporting reports

You can export a report by clicking the ⬇ icon in the **View Result** window to export the report. A zip file is generated containing separate folders for configuration and performance reports. (For reports that include just configuration metrics, only the conf folder is included in the zip file.)

Using a saved query

Saved queries are displayed in the Saved Queries section in Report Builder. You can view, edit, clone, and delete saved queries.

Build

Create New Query

 Create Using Query Builder >

 Create Using MQL >

Saved Queries (22)

Search Queries

 LDEV (421358-00:00:05) - Total IOPS and Response Time	24/09/19 09:40	 
 Enterprise Storage 421358 - Cache Utilization	24/09/19 09:41	 
 LDEV Total IOPS	25/09/19 12:34	 

Viewing or editing a query

You can view a saved query to see its details, such as resources and filters. You can also edit the saved query to add or remove resources and filters.

Procedure

1. In the **Build** window, in **Saved Queries** section, click  in the **Action** column.
The query details are displayed. You can add, remove, edit, or hide the resources and filters.
2. If you edited the query, click **View Result** and then click **Save Query**.

Cloning a query

Cloning a query is useful to extend existing queries and save as a new query.



Note: You can clone the queries that are created using the Query Builder option.

Procedure

1. In the **Build** window, in **Saved Queries** section, click  in the **Action** column.
The query details are displayed.
2. Click **Clone Query**.
The **Clone Query** window opens.
3. In the **Query Name** box, enter a new name.
4. Click **Clone**.
The confirmation message is displayed.
5. Make the desired changes.
6. Click **View Result**.
The **View Result** window opens.
7. Click **Save Query** and then click **Save**.

Deleting a query

You can delete saved queries.

Procedure

1. In the **Build** window, go to the **Saved Queries** section and click  in the **Action** column.
A confirmation message is displayed.
2. Click **Delete**.
The query is removed from the **Saved Query** section.

Chapter 7: Administering Analyzer detail view

There are several administrative tasks that are related to the operation of Analyzer detail view.

Resetting a forgotten Analyzer detail view password

You can reset a password with the Reset Password link in the Analyzer detail view Logon window. Active directory users must reset (change) their password through the Active Directory.

Procedure

1. In the **Logon** window, click **Reset Password**.
2. In the **Upload License for User Authentication** window, upload the license file, and then click **Submit**.
The **Reset Password** window opens.
3. Type your user name and the new password.
The password must be a minimum of six characters with the following requirements:
 - One uppercase letter and one lowercase letter
 - One number and one special character. The following special characters are supported:
!, ' , ` , @ , # , \$, % , ^ , & , * , (,) , - , _ , + , =
4. Click **Submit**.
The system verifies the license and shows the success message.
5. Click **Login** to log on to the Analyzer detail view.

Checking the Analyzer detail view status

You can view the status of the host system (Analyzer detail view).

Monitoring Analyzer detail view alerts

The System Alerts tab in the detail view GUI allows you to subscribe to alerts regarding operation of the Analyzer detail view. (These alerts are separate from the resource alerts.)

The System Alerts tab lists the following resources.

Resources	Threshold values	Monitor interval
Downloader Delay	> 30 minutes	every 15 minutes
Import Delay	> 300 minutes (Configuration)	every 15 minutes
	> 30 minutes (Performance)	every 15 minutes
License Expiration	Before 15 days	every day (12 AM)
System Memory Usage	> 80%	every 30 minutes

System resources are monitored at the defined interval, and a violation is reported to the Syslog server or registered email address.

If you have configured the Syslog server to receive system alerts messages, then an alert notification is sent for each violation.

If you have subscribed to email alerts, then a notification is sent to the registered email address or group only if there is a status change from green to red (or red to green).

To subscribe to the system alerts, follow these steps:

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the application bar area, click the **Alerts** menu, and select **Definitions**.
3. Select the **System Alerts** tab.
4. Click **Subscribe**, select the alert you want to subscribe to, and supply the email or Syslog server information.

Changing thresholds for detail view system alerts

You can change the default value of the alert thresholds for Analyzer detail view resources.

Procedure

1. In the application bar area, click the **Alerts** menu, and select **Definitions**.
2. Select the **System Alerts** tab.
3. Select a system alert, and then click **Edit**.
4. Change the threshold, and then click **Save**.

Viewing the system status (operating system)

The System Status options in the detail view GUI display the health of the Analyzer detail view by displaying information about CPU utilization, RAM usage, swap rate, disk usage, and

so on. The System status helps to diagnose and change the configuration of RAM, data processes, and the CPU.

Procedure

1. Log on to the Analyzer detail view as the `admin` user.
2. In the application bar, click the **Manage** menu.
3. In the **Manage** window, in the **Status** section, click the **System Status** link.
4. When the **System Status** is displayed, view the system status.

Viewing for detail view data processing status

Ops Center Analyzer detail view collects data from the FTP server at regular intervals. Use the **Status** window of the detail view GUI to review the status of data download, import, and report generation.

Access Analyzer detail view from the More Actions menu.

Click the Server Status icon (exclamation point) in the application bar area. The color of the icon represents the overall status of Analyzer detail view data processing.

- **Green:** The data was processed successfully.
- **Red:** An alert occurred at the FTP server, probe importer, or during report generation.

Data Download Status

Column name	Description
Probe server	IP address of the Analyzer probe server. If you are using multiple network interface cards (NIC) in the Analyzer probe server, the IP address might not show as expected; however, this does not impact the operation of the Analyzer detail view server.
Appliance ID	Name of the directory on the FTP server where the probe uploads the data. If the data is uploaded directly to the Analyzer detail view server, then the directory is created on the Analyzer detail view server, and the Analyzer detail view server downloads the data from this directory. If the Analyzer detail view server does not receive any data from an Analyzer probe server for 30 days, the server is considered inactive and is not displayed in the appliance list. If data is subsequently received from an inactive server, it is again displayed in the appliance list.
Status	Status of the data download appears in one of two colors: ▪ Green: The download from the FTP server was successful. ▪ Red: The download failed. A possible cause is a delay in sending the data from the probe to the FTP server, or the Analyzer detail view server cannot connect to the FTP server.
FTP server	Name of the FTP server.

Column name	Description
Last Downloaded File's Time Stamp	Time of the previous data download.
Data Available Until	Time until when the data or logs are available on the FTP server.

Data Import Status

Column name	Description
Probe Type	Type of Hitachi or third-party probe.
Status	Status of the data processing of the probe: ▪ Green: The data processing was successful. ▪ Red: The data processing failed for one or more probes. A possible cause is the Analyzer detail view server does not receive the configuration or performance data in the scheduled time. The Analyzer detail view server must receive the configuration data in 4 hours and performance data in 20 minutes.
Probe Name	Name of the probe for which data is sent to the Analyzer detail view server.
Probe Server	IP address of the Analyzer probe server. If you are using multiple network interface cards (NIC) in the Analyzer probe server, the IP address might not show as expected; however, this does not impact the operation of the Analyzer detail view server.
Last Configuration Import Time	Time when the configuration data was processed.
Last Performance Import Time	Time when the performance data was processed.

Real Time Probes

Column name	Description
Probe Type	Type of Hitachi or third-party probe.

Column name	Description
Status	Status of the real-time data processing of the probe: ▪ Green: The real-time data processing was successful. ▪ Red: The real-time data processing failed for one or more probes. A possible cause is the Analyzer detail view server does not receive the real-time data in the scheduled time.
Probe Name	Name of the probe for which data is sent to the Analyzer detail view server.
Probe Server	IP address of the P address of the Analyzer probe server. If you are using multiple network interface cards (NIC) in the Analyzer probe server, the IP address might not show as expected; however, this does not impact the operation of the Analyzer detail view server.
Last Performance Collection Time	Time when the real-time data was collected.

Viewing the status of detail view add-on applications

The App Status window of the detail view GUI shows the status of any add-on applications on the Analyzer detail view.

Procedure

1. Log on to the Analyzer detail view as the `admin` user.
2. In the application bar, click the **Manage** menu.
3. Click **App Status**.
The window lists the details such as application name, version, and type.

Downloading Analyzer detail view diagnostic data

The Analyzer detail view collects various log files that are useful for troubleshooting. The Download Diagnostic Data feature provides the facility to download these files in an archive file. If you cannot resolve the problem, send the generated data file with the error messages to the customer support for analysis.

Procedure

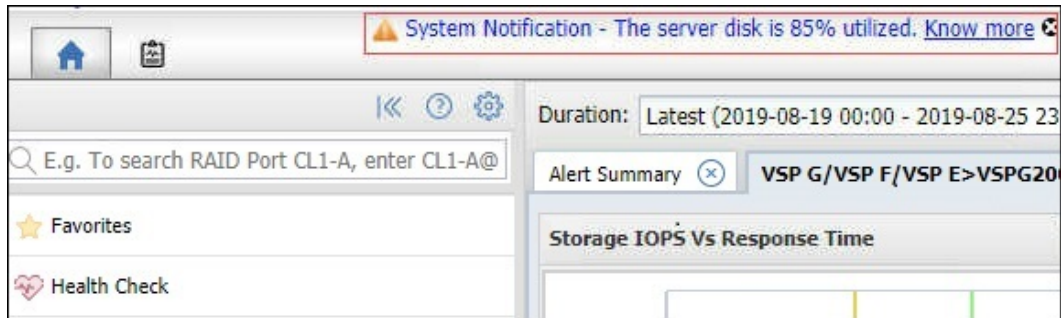
1. Log on to the Analyzer detail view as the `admin` user.
2. In the application bar, click the **Manage** menu.
3. In the **Administration** section, click **Download Diagnostic Data**.
4. In the **Download Diagnostic Data** window, click **OK**.
The system initiates the diagnostic data generation process.

5. Click **Download**.

Sample diagnostic data file name: diag_server_20190807011147.gz

System notifications

The system notifications are displayed in the UI for certain critical events, such as when disk utilization is high or disk space is becoming critical.



Managing Analyzer detail view user accounts

The administrator user can create multiple users in Ops Center Analyzer detail view with different access rights (permissions). The Analyzer detail view and Analyzer probe also provides an option to Active Directory administrator users to restrict the access of UI to only Active Directory users.

The administrator can create the following types of users:

- **Local:** This user is created in Analyzer detail view and Analyzer probe by assigning the user ID, password, locale, email and so on.
- **Active Directory:** This user is created in the Active Directory. To add this user, you need the active directory domain name and user name. The group, email, and locale can be assigned to this user. After adding a user in Analyzer detail view and Analyzer probe, the Active Directory user can access Analyzer detail view and Analyzer probe by using the assigned password. Active Directory support was tested on schema version 56 with Microsoft Windows Server 2012.
 - If the SSL port is enabled and the non-SSL port is disabled to connect to the Active Directory server, see [Configuring the SSL port \(on page 122\)](#).
 - To add the Active Directory user, the Active Directory domain name must be resolved by the Analyzer detail view and Analyzer probe. See [Verifying the Active Directory domain name \(on page 124\)](#).
 - If you are using a non-default setting to connect to the Active Directory server, see [Matching non-default Active Directory server settings \(on page 124\)](#).
 - The supported authentication and communication protocols for Active Directory are as follows:
 - Authentication protocol: LDAP
 - Communication protocols:
 - For TLS/SSL: LDAPS
 - Without SSL: Plain text (non-TLS)

Editing a user

You can only edit the language (locale) and the email address.

Procedure

1. In the application bar, click the **Manage** menu.
2. In the **Administration** section, click the **Manage Users** link.
The **Manage Users** window appears.
3. Click the **Edit** link and click **Submit**.

Deleting a user

Procedure

1. In the application bar, click the **Manage** menu.
2. In the **Manage** window, in the **Administration** section, click the **Manage Users** link.

3. In **Action**, click the **Delete** link.
The confirmation message appears.
For example, users with Active Directory type and with Administrator rights (permissions) cannot delete their own profile, but can delete the Active Directory and local user types.
4. Click **OK**.

Changing a password

Procedure

1. In the application bar, click the **Manage** menu.
2. In the **Manage** window, in **Administration**, click the **Manage Users** link.
The **Manage Users** window opens.
3. In **Action**, click the **Change Password** link, and then change the password.
The password must be a minimum of six characters, with the following conditions:
 - You cannot reuse your previous six passwords.
 - Passwords cannot contain a user name.
 - Passwords must contain one uppercase letter and one lowercase letter.
 - Passwords must contain one digit and one special character. The following special characters are supported:

!, ', ` , @, #, \$, %, ^, &, *, (,), -, _ , +, =



Note: These password requirements do not apply to Active Directory users.

- You cannot change the password of the Active Directory users. It must be changed in the Active Directory. For example, users with the Active Directory type and Administrator rights (permissions) cannot change their own password and other Active Directory user passwords, but can reset the password of other local users.
4. Click **Submit**.

Resetting a password

Procedure

1. In the application bar, click the **Manage** menu.
2. In the **Manage** window, in **Administration**, click the **Manage Users** link.
The **Manage Users** window opens.
3. In **Action**, click the **Reset Password** link.
4. The confirmation message appears. Click **Ok**.
The user password is reset and shown on the UI.
Sample reset password message:
Password has been successfully reset to 4n1T9P\$fd
5. Copy the password and click **OK**.



Note: You cannot reset the password of the Active Directory users. Reset it in Active Directory. For example, users with an Active Directory type and Administrator rights (permissions), cannot reset their own password and other Active Directory users, but can reset the password of local users.

Restricting UI access to Active Directory users

You can enhance the security of the Analyzer detail view and Analyzer probe UI by restricting the access to Active Directory users only. Any Active Directory administrator user can apply this restriction by enabling **Allow Access to Active Directory users only** option. After enabling this option only the Active Directory users can access the Analyzer detail view and Analyzer probe UI.

Before you begin

At least one Active Directory administrator user must be present on the Analyzer detail view and Analyzer probe to enable the **Allow Access to Active Directory users only** option.



Note: You must enable the Allow Access to Active Directory users only option separately on Analyzer detail view and Analyzer probe.

Procedure

1. Log on to the Analyzer detail view or Analyzer probe as an Active Directory administrator user.
2. In the application bar, click the **Manage** menu.
3. In the **Manage** window, in the **Administration** section, click the **Manage Users** link.
4. Select the **Allow Access to Active Directory users only** check box. (To disable **Allow Access to Active Directory users only** option clear the check box.)

After enabling this option Local users (administrator or normal) cannot access the Analyzer detail view or Analyzer probe.

The following table describes the access rights after enabling the strict Active Directory mode.

User type	Group	Rights	
		REST API	Access to Analyzer detail view and Analyzer probe UI
Active Directory	Administrator	Yes	Yes
	Normal	Yes	Yes
Local	Administrator	No	No
	Normal	No	No

Active Directory settings

The following procedures support Active Directory settings in Analyzer detail view and Analyzer probe.

The supported authentication and communication protocols for Active Directory are as follows:

- Authentication protocol: LDAP
- Communication protocols:
 - TLS/SSL: LDAPS
 - Without SSL: Plain text (non-TLS)

Configuring the SSL port

The SSL port is enabled and the non-SSL port is disabled while connecting to the Active Directory server.

Before you begin



Note: If you do not want to stop the `crond` service, you can stop specific processes of the Analyzer detail view server and Analyzer probe server by using the `crontab -e` command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 153\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 154\)](#)

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like `putty`) as a root user.
2. From the Analyzer detail view server or Analyzer probe server, verify the domain name of the Active Directory using the command:

```
nslookup domain-name
```

3. If you cannot resolve the domain name, then add an entry of the following form in the `/etc/hosts` file:


```
Active-Directory-server-IP-address domain-name
```
4. Import one of the following certificates into the Analyzer detail view server or Analyzer probe server keystore:



Note: The password for the keystore is `changeit`.

- Active Directory Server certificate (CER format).
 - Microsoft Public Key Infrastructure (MSPKI) chain Certificate (CER format), one file that contains all the keys.
5. Upload the CER file at the following location `/tmp` on the Analyzer detail view server or Analyzer probe server using an FTP client (like WinSCP).
 6. Navigate to the Java keystore directory. For example:

```
/usr/lib/jvm/java-17-amazon-corretto/lib/security
```

7. If the `jssecacerts` file does not exist, create it.

8. Import the certificate into the Analyzer detail view server or Analyzer probe server using the command:

```
keytool -importcert -alias Alias_name -keystore Truststore_file_path -storetype
jks -storepass Truststore_file_password -file
Active_Directory_Server_certificate_or_MSPKI_chain_certificate_file_path
```



Note: You can define any unique alias name for the certificate.

For example:

```
keytool -importcert -alias detailviewAD -keystore jssecacerts -storetype jks -
storepass changeit -file /tmp/LAB_chain.cer
```

9. Make sure that the megha user has the read permission for the `jssecacerts` file. If not, change the permission as follows.

For example:

```
chmod o+r jssecacerts
```

10. Stop the crond service and verify the status:

```
service crond stop
```

```
service crond status
```

11. Stop the megha service and verify the status:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

```
/usr/local/megha/bin/megha-jetty.sh status
```

12. Start the megha service and verify the status:

```
/usr/local/megha/bin/megha-jetty.sh start
```

```
/usr/local/megha/bin/megha-jetty.sh status
```

13. Start the crond service and verify the status:

```
service crond start
```

```
service crond status
```



Note: If you upgrade the JDK in the future, make sure that the `jssecacerts` file is copied to the upgraded JDK directory.

For example: If you upgrade JDK from v1.8.0 to v17, copy the `jssecacerts` file from `/usr/java/jdk1.8.0_291-amd64/jre/lib/security` to `/usr/lib/jvm/java-17-amazon-corretto/lib/security`.

After copying the `jssecacerts` file, make sure that megha user has the read permission for the `jssecacerts` file. If not, set it as in this example:

```
chmod o+r jssecacerts
```

14. Access the Analyzer detail view or Analyzer probe UI as an administrator user, and then add the Active Directory users.

Verifying the Active Directory domain name

Before you can add an Active Directory user, the Active Directory domain name must be resolved by the Analyzer detail view server or Analyzer probe server.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like `putty`) as a root user.
2. Verify the domain name of the Active Directory using the following command:

```
nslookup domain-name
```

3. If you cannot resolve the domain name, then add an entry of the following form in the `/etc/hosts` file:

```
Active-Directory-server-IP-address domain-name
```

Matching non-default Active Directory server settings

If you are using a non-default setting to connect to the Active Directory server, you must follow this procedure to change the settings on the Analyzer detail view server and Analyzer probe server

The default non-SSL port is 389 and the SSL port is 636.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like `putty`) as a root user.
2. List the details of the properties using the command:

```
cat /usr/local/megha/conf/sys/ad.properties
```

The default values are:

- `ad.ssl.port=636`
- `ad.non.ssl.port=389`
- `ad.auth.type=simple`
- `ad.connect.timeout=5000`
- `ad.connect.retry.interval=1000`
- `ad.connect.retry.times=2`



Note: The `simple` authentication type is supported for `ad.auth.type` property.

3. Note any property value that needs to be changed. For example, `ad.ssl.port=123`.
4. Enter the command:

```
cd /usr/local/megha/conf
```

5. Create a new custom directory as follows:

```
mkdir custom
```

6. Create a file `custom.properties` in the new folder you just created (`/usr/local/megha/conf/custom`).
7. In the `custom.properties` file, add the property you noted earlier. For example:
`ad.ssl.port=123`.
8. Change the owner of the new files and folders:

```
chown -R megha:megha /usr/local/megha/conf/custom
```

9. Stop the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh stop
/usr/local/megha/bin/megha-jetty.sh status
```

10. Start the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh start
/usr/local/megha/bin/megha-jetty.sh status
```

Setting an explicit domain name for Active Directory

To enhance the security, you can use an explicit User Principal Name (UPN) domain name on the Analyzer detail view server and Analyzer probe server.



Note: If you do not want to stop the `crond` service, you can stop specific processes of the Analyzer detail view server and Analyzer probe server by using the `crontab -e` command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 153\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 154\)](#)

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like `putty`) as a root user.
2. Stop the `crond` service and verify the status with these commands:

```
service crond stop
service crond status
```

3. Stop the `megha` service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh stop
/usr/local/megha/bin/megha-jetty.sh status
```

4. Go to the `/usr/local/megha/conf` directory:

```
cd /usr/local/megha/conf
```

5. (If the `custom` directory does not exist) create it as follows:

```
mkdir custom
```

6. (If the `custom.properties` file does not exist), create it in the `custom` directory.
7. Change ownership of the `custom` directory:

```
chown -R megha:megha /usr/local/megha/conf/custom
```

8. Open the `custom.properties` file and add the `ad.domain.mappings` property with the implicit and explicit domain name:

```
ad.domain.mappings=Explicit_Domain:Implicit_Domain
```

For example:

```
ad.domain.mappings=marsh.com:domain1.com
```

To map multiple explicit domain names, separate them with commas:

For example:

```
ad.domain.mappings=marsh.com:domain1.com,marsh1.com:domain1.com
```

9. Save the changes.

10. Start the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh start
/usr/local/megha/bin/megha-jetty.sh status
```

11. Start the crond service and verify the status with these commands:

```
service crond start
service crond status
```

Managing Active Directory groups

You can add Active Directory groups to the Analyzer detail view or Analyzer probe. (To log on to the server Ops Center Analyzer detail view as an Active Directory user, the Active Directory user must be a member of the Active Directory group and domain).

Procedure

- Log on to the Ops Center Analyzer detail view as the `admin` user and make the appropriate selection:
 - Analyzer detail view:** In the application bar, click the **Manage** menu.
 - Analyzer probe:** Click the **Manage** menu.
- In the **Administration** section, click the **Manage Active Directory Groups** link.
- In the **Manage Active Directory Groups** window, click **Add Active Directory Group**.
- Type the Active Directory group name and domain name.



Note: If you have configured an explicit domain name for Active Directory using the `ad.domain.mapping` property, make sure that you enter the explicit domain name in the **Domain Name** field. Refer to [Setting an explicit domain name for Active Directory \(on page 125\)](#) for more information.

- Type the user name (with the fully qualified domain name) and the password. You must type the username in the following format:

`user-name@FQDN`

For example: `smith@corp.company`



Note: The Active Directory group user can log in to the Analyzer detail view or Analyzer probe using the `user-name@FQDN` and `FQDN\user-name` formats. The `NetBIOS-Name\user-name` format is not supported.

All users from the specified Active Directory group are registered with Analyzer detail view (as Normal users) or Analyzer probe (as Admin users) and can access the UI by using the Active Directory logon credentials.

- Click **Submit**.

Editing the Active Directory group domain name

You can edit the Active Directory group domain name on the Analyzer detail view or Analyzer probe servers. (To log on to the Analyzer detail view server as an Active Directory user, the user must be a member of the Active Directory groups and domains).

Procedure

1. Log on to the Ops Center Analyzer detail view as the `admin` user and make the appropriate selection:
 - **Analyzer detail view:** In the application bar, click the **Manage** menu.
 - **Analyzer probe:** Click the **Manage** menu.
2. In the **Administration** section, click the **Manage Active Directory Groups** link.
3. In the **Manage Active Directory Groups** window, click **Edit** in the **Action** column.
4. Edit the domain name.



Note: If you have configured an explicit domain name for Active Directory using the `ad.domain.mapping` property, make sure that you enter the explicit domain name in the **Domain Name** field. Refer to [Setting an explicit domain name for Active Directory \(on page 125\)](#) for more information.

5. Type the user name (with the fully qualified domain name) and the password. You must type the username in the following format:

`user-name@FQDN`

For example: `smith@corp.company`



Note: The Active Directory group user can log in to the Analyzer detail view or Analyzer probe using the `user-name@FQDN` and `FQDN\user-name` formats. The `NetBIOS-Name\user-name` format is not supported.

All users from the specified Active Directory group are registered with Analyzer detail view (as Normal users) or Analyzer probe (as Admin users) and can access the UI by using the Active Directory logon credentials.

6. Click **Submit**.

Disabling validation for Active Directory sAMAccountName and domain

You can change settings to disable validation for Active Directory sAMAccountName and domain.



Note: If you do not want to stop the `crond` service, you can stop specific processes of the Analyzer detail view server and Analyzer probe server by using the `crontab -e` command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 153\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 154\)](#)

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like `putty`) as a root user.
2. Stop the `crond` service and verify the status with these commands:

```
service crond stop
service crond status
```

3. Stop the `megha` service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh stop
/usr/local/megha/bin/megha-jetty.sh status
```

4. Go to the `/usr/local/megha/conf` directory:

```
cd /usr/local/megha/conf
```

5. (If the `custom` directory does not exist) create it as follows:

```
mkdir custom
```

6. (If the `custom.properties` file does not exist), create it in the `custom` directory.
7. Change ownership of the `custom` directory:

```
chown -R megha:megha /usr/local/megha/conf/custom
```

8. Open the `custom.properties` file and add the following properties:

- To disable validation for `sAMAccountName`:

```
ad.validate.username=false
```

- To disable validation for domain:

```
ad.validate.domain=false
```

9. Save the changes.
10. Start the `megha` service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh start
/usr/local/megha/bin/megha-jetty.sh status
```

11. Start the `crond` service and verify the status with these commands:

```
service crond start
service crond status
```

Changing the built-in FTP (meghadata) user password

Ops Center Analyzer detail view uses a built-in FTP server to transfer data from Analyzer probe server to Analyzer detail view server. The FTP server in Ops Center Analyzer detail view comes with a built-in user (username: meghadata). You can change the meghadata user's password if required, from the Analyzer detail view GUI.

Procedure

1. In the application bar, click the **Manage** menu.
2. In the **Manage** window, in **Administration**, click the **FTP User Password** link.
3. In the **FTP User Password** window, enter the required details to change the password. (Password can contain any characters except for the following: Single quotation mark ('), multiple spaces in between, and space at the beginning and end.)

After changing the password, make sure that you update the password on the Analyzer probe UI, which is used for connecting the Analyzer probe server and Analyzer detail view server.

To change the password on the Analyzer probe UI, go to the **Home > Reconfigure > Analyzer detail view server** tab.

Managing detail view email groups

Follow these procedures to create email groups.

Creating email groups in detail view

You can create a group of email addresses to send alert notifications for detail view . You can view this when you add alerts in the Add Alerts > Alerts Notification section and in Alerts Definition > Subscribe Alerts of the detail view GUI.

Procedure

1. Select **Tools > Data Center Analytics** to start the detail view GUI.
2. In the application bar, click the **Manage** menu.
3. In the **Manage** window, in **Administration**, click the **Manage Email Groups** link.
4. In the **Email Groups** window, click **Add Group**.
5. In the **Add Email Group** window, provide the group name and email addresses. (To add multiple email addresses, press **Tab** or **Enter**.)
6. Click **Save**.

Editing and deleting email groups in detail view

You can edit, add, and delete an email address from an existing email group, or delete an email group.

Procedure

1. Select **Tools > Data Center Analytics** to start the detail view GUI.
2. In the application bar, click the **Manage** menu.
3. In the **Manage** window, in **Administration**, click the **Manage Email Groups** link. The **Email Groups** window opens.
4. In **Action**, click:
 - **View**: To view the members of the group.
 - **Edit**: To edit the group details. You can add a new email address to the group, or delete an existing email address. Click **Save** when your changes are complete.
 - **Delete**: To delete the email group. Click **Yes** at the confirmation message.

Adding a disclaimer or banner message to the Analyzer detail view login window

You can add a custom login message to the Analyzer detail view. This helps you add a specific message that needs the user's attention before login.

Procedure

1. Log on to the Analyzer detail view as the `admin` user.
2. In the application bar, click the **Manage** menu.
3. In the **Manage** window, in the **Settings** section, click the **Disclaimer** link. The **Disclaimer** window opens.
4. In the **Disclaimer** window, select the **Show Disclaimer** check box.
5. In the disclaimer text area, type the disclaimer text.
6. Click **Update**.

Changing the Analyzer detail view locale

Only the U.S. English locale is supported.

Setting the Analyzer detail view time zone

Set the time zone of Analyzer detail view at the time of deployment. All the reports are in this time zone.

If the Analyzer detail view is in the India Standard Time (IST) time zone, one storage system is in the Eastern U.S. time zone, and another storage system is in the Central U.S. time zone, the reports of both storage systems display in the IST time zone.

To change the time zone according to the storage systems time zone, use this feature. This time zone applies to each storage system report.

Procedure

1. Log on to the Analyzer detail view as the `admin` user.
2. In the application bar, click the **Manage** menu.
3. In the **Manage** window, in the **Settings** section, click the **Set Time Zone** link.
The **Set Time Zone** window opens.
4. Select **Time Zone** and click **Submit**.

Managing the Analyzer detail view database size

You can manage the size of the Analyzer detail view database based on time (age of the data), current size, and amount of available disk space. You can put limits on the performance database to purge the performance data. (You cannot purge the configuration data.)

On the Analyzer detail view server, the performance data is stored in: `/usr/local/megha/db/perf/date` (the date format is: YYYYMMDD).

Each *date* folder contains performance data for one day.

You can also manage the size of the backup and meghadata directories based on time (age of data).

Controlling the size of the performance database

You can control the size of the performance database by setting values in the `/usr/local/megha/conf/sys/app.db.purge.properties` file.

The database purging activity is scheduled daily at 00:00 UTC. However, the purging activity starts only when the Analyzer detail view server is not performing any of the following operations:

- REST API requests
- Data batch importing
- UI activities that require database access



Note: While purging activity is in progress, you cannot access the database.

You must set the following property to true when enabling purging activity:

`app.db.purging.enabled`

In addition, you must set one of the following properties:

- Time (`app.db.time.based.purging.limit`)
- Size (`app.db.size.based.purging.limit.in.gb`)
- Disk free space (`app.disk.freespace.size.based.purging.limit.in.gb`)

If you set more than one property, then only the highest configured criteria will be applied and further criteria will be skipped. The Disk free space purging is the highest priority. Size purging is a higher priority than Time.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Type the following properties file path:
/usr/local/megha/conf/sys/app.db.purge.properties
3. Set the values according to the settings described in the following table.

Parameter	Values	Description
app.db.purging.enabled	true, false Default: false	Enable or disable database purging.
app.db.time.based.purging.limit	nD (days, Min: 7, Max: 3650) nM (months, Min: 1, Max: 120) nY (years, Min:1, Max: 10)	Purge based on database age (days, months, or years). Example: app.db.time.based.purging=10M Saves the last 10 months of data.
app.db.size.based.purging.limit.in.gb	Min: 50 Max: 10240	Purge based on the database size (in GB). Deletes oldest folders in <code>perf</code> until the database size limit is reached. Example: app.db.size.based.purging.limit.in.gb=100 Deletes the oldest folders until the database size is less than or equal to 100 GB.
app.disk.freespace.size.based.purging.limit.in.gb	Min: 10 Max: 100	Purge database based on the amount of free disk space available (in GB). Deletes the oldest folders in <code>perf</code> until the free disk space limit is reached. Example: app.disk.freespace.size.based.purging.limit.in.gb=20 Deletes the oldest folders until the amount of free disk space is less than or equal to 20 GB.



Note: If you make any change in the property file, then you must restart the Analyzer detail view server. If you type an incorrect value in the property file, then the Analyzer detail view server does not restart. The Analyzer detail view server updates the `importStatus.properties` file after the database purge operation and lists the correct data availability.

Controlling the size of the backup directory

You can control the size of the backup directory by setting values in the `megha_cleanup_custom.properties` file. The backup directory purging activity is scheduled daily at 00:10 hours. By default, the data is retained for 30 days.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.

2. Type the following properties file path:

```
cd /usr/local/megha/conf/
```

3. Create a backup copy of the `megha_cleanup_custom.properties` file using the following command:

```
cp megha_cleanup_custom.properties bkp_megha_cleanup_custom.properties_bkp
```

4. Open the `megha_cleanup_custom.properties` file using a text editor (such as **vi**) and change the following properties:

```
cleanupapp.db.backup.root=/usr/local/megha/db/backup
cleanupapp.db.backup.enable=yes
cleanupapp.db.backup.retentiontime=30 #value in days
```

Controlling the size of the meghadata directory

You can control the size of the meghadata directory by setting values in the `meghadata_cleanup_custom.properties` file. The meghadata directory purging activity is scheduled daily at 00:10 hours. By default, the data is retained for 90 days.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.

2. Enter the following command:

```
cd /usr/local/megha/conf/
```

3. Create a backup copy of the `meghadata_cleanup_custom.properties` file using the following command:

```
cp meghadata_cleanup_custom.properties
bkp_meghadata_cleanup_custom.properties_bkp
```

4. Open the `meghadata_cleanup_custom.properties` file using a text editor (such as `vi`) and change the following properties:

```
cleanupapp.client.zip.root=/home/meghadata/**-**-**-**
cleanupapp.client.zip.enable=yes
cleanupapp.client.zip.retentiontime=90 #value in days
```



Note: Do not change the value of the `cleanupapp.client.zip.retentiontime` property to less than 5 days.

Viewing and updating the Analyzer detail view license

You can view the current license information (including the licensed monitoring capacity), or add new licenses.

Procedure

1. Log on to the Analyzer detail view as the `admin` user.
2. In the application bar, click the **Manage** menu.
3. In the **Manage** window, in the **Status** section, click the **License Information** link. The **License Information** window displays all the configured licenses including identifier, key code, key limit, license usage, total license value, date range, and status. The identifier is used as a unique ID for Hitachi storage systems. The criteria for license can be capacity or count.
 - You can check the Usage and Value columns to verify that you have license nodes available.
 - In the case of license expiration or adding a new license, you can upload the license file using the **Select File** and **Submit** buttons.



Note: If you delete a probe or stop monitoring a target, the license count in the Usage column is decreased next time the configuration data is updated.

Resolving the SMTP connection for detail view

Before configuring the SMTP server, verify if the Analyzer detail view server can resolve the SMTP host name.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like `putty`) as a root user.

2. Verify if the Analyzer detail view server can resolve the SMTP host name, using the following command:

```
nslookup hostname
```

3. If you cannot resolve the domain name, then add an entry of the following form to the `/etc/hosts` file:

```
ipaddress hostname
```

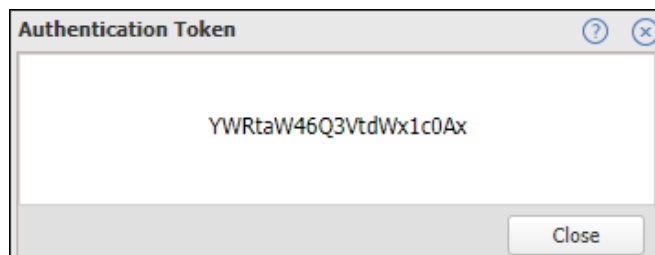
Using the detail view authentication token

You need an authentication token to make a Analyzer detail view REST API request.

Because the API request uses HTTP basic authorization, you must use this authentication token with every request.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.
2. In the application bar, click the **Manage** menu.
3. In the **Administration** section, click the **Authentication Token** link.
The **Authentication Token** window shows the token.



Note: If you have logged on to the Analyzer detail view using an Active Directory account, the **Enter password for active directory user** window opens. Provide the password and then click **Submit**.

4. If you want to change the token, change the user password. The token is updated automatically.
5. To view the new authentication token, click the **Manage** menu, and then in the **Administration** section, click the **Authentication Token** link.

Viewing the Analyzer detail view schema

You can view the complete schema used by the Analyzer detail view database.

Procedure

1. Access Analyzer detail view from the **More Actions** menu.

2. In the application bar, click the **Manage** menu.
3. In the **Administration** section, click the **Show Schema** link.
The **Show Schema** window opens, displaying the details of all the attributes, resource definitions, and relationships.

Contents of the MIB file on the Analyzer detail view

The Analyzer detail view sends notifications in the form of traps to the SNMP Manager. The trap structure is defined in a Management Information Base (MIB) file. You can download the MIB file from **Manage > Download SNMP MIB File**. A zip file is downloaded, which contains separate MIB files for the SNMP versions (v1, v2C, and v3). The file content of these three versions is similar.

The contents of the MIB objects are as follows:

```
iso(1).org(3).dod(6).internet(1).private(4).enterprise(1)
|
hitachi(116)
+-----+
systemAP(7)                systemExMib(5)
|                           |
performanceAnalytics(63)    performanceAnalyticsExMib(63)
|                           |
performanceManagement(12)   performanceManagementExMib(12)
|                           |
performanceManagementTrap(2) performanceManagementTrapExMib(2)
```

Contents of the MIB objects.

Object ID	Name	Description
.1.3.6.1.4.1.116.5.63.12.2.2	resourceName	Name of the target resource that has violated the threshold.
.1.3.6.1.4.1.116.5.63.12.2.4	resourceSignature	Signature of the target resource that has violated the threshold.
.1.3.6.1.4.1.116.5.63.12.2.5	metric	Name of the metric that has violated the threshold.
.1.3.6.1.4.1.116.5.63.12.2.6	categoryNameAndConditionalExpression	Alert condition expression.
.1.3.6.1.4.1.116.5.63.12.2.7	alertValue	List of violated values for alert violations in the assessment period.

Object ID	Name	Description
.1.3.6.1.4.1.116.5.63.12.2.8	alertSeverity	Severity of the alert: Normal, Warning, or Critical
.1.3.6.1.4.1.116.5.63.12.2.9	probeType	The probe type of the target resource that has violated the threshold.
.1.3.6.1.4.1.116.5.63.12.2.11	threshold	Threshold value that is defined while creating the alert.
.1.3.6.1.4.1.116.5.63.12.2.12	probeld	The probe ID of the target resource that has violated the threshold.
.1.3.6.1.4.1.116.5.63.12.2.13	alertMessage	The descriptive alert message containing details of the violation.
.1.3.6.1.4.1.116.5.63.12.2.15	alertName	Alert name defined in the created alert.
.1.3.6.1.4.1.116.5.63.12.2.16	serverName	The Analyzer detail view server name or IP address.
.1.3.6.1.4.1.116.5.63.12.2.17	assessmentFrom	Start timestamp for the violation.
.1.3.6.1.4.1.116.5.63.12.2.18	assessmentTo	End timestamp for the violation.
.1.3.6.1.4.1.116.5.63.12.2.19	violationTimestamps	List of timestamps for alert violations in the assessment period.
.1.3.6.1.4.1.116.5.63.12.2.20	probeServer	The Analyzer probe server name or IP address from which the resource data is collected.
.1.3.6.1.4.1.116.7.63.12.2.10	performanceManagementTrap-NORM	Trap sent when the alert severity is Normal
.1.3.6.1.4.1.116.7.63.12.2.20	performanceManagementTrap-WARN	Trap sent when the alert severity is Warning
.1.3.6.1.4.1.116.7.63.12.2.30	performanceManagementTrap-CRIT	Trap sent when the alert severity is Critical
.1.3.6.1.4.1.116.7.63.12.2.40	performanceManagementTrap-TEST	Trap sent for a test connection.

Configuring an SSL certificate (Analyzer detail view server)

Configure an SSL certificate to initiate a secure browser sessions. You can either configure the CA signed or self-signed SSL certificate.

Configuring a CA signed SSL certificate (Analyzer detail view server)

Configure a CA signed SSL certificate to initiate a secure browser sessions by creating a private key, creating a certificate signing request (CSR), and applying the server certificate.

Creating a private key and a certificate signing request

Create a certificate signing request (CSR) for Analyzer detail view server and send it to the certificate authority to obtain the certificate file.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Navigate to the `/usr/local/megha/jetty/etc` directory:

```
cd /usr/local/megha/jetty/etc
```

3. Create a private key using one of the following algorithms:

RSA:

```
openssl genrsa -out jettyPrivate.key
```

ECDSA:

```
openssl ecparam -out jettyPrivate.key -name prime256v1 -genkey
```

4. Create a certificate signing request (CSR):

```
openssl req -new -key jettyPrivate.key -out /tmp/certreq.csr
```

Follow the instructions displayed on the console to enter the details for your certificate request. When requested to provide the common name, make sure that you enter a fully qualified host name.

Enter the default password for CSR: `megha.jeos`



Note: If you provide a password of your choice, note it. You will need this when applying server certificates.

5. Copy the certificate request file from `/tmp/certreq.csr` and submit it to the certificate authority to create the certificate file.

Applying server certificates

The certificate authority creates the following three certificate files:

- Root
- Intermediate
- Host



Note: If you do not want to stop the `crond` service, you can stop specific processes of the Analyzer detail view server and Analyzer probe server by using the `crontab -e` command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 153\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 154\)](#)

Procedure

1. Upload the certificate files to the Analyzer detail view server. (For example, `/usr/local/megha/jetty/etc`).
2. Navigate to the `/usr/local/megha/jetty/etc` directory:

```
cd /usr/local/megha/jetty/etc
```

3. Combine the chain of certificates by concatenating them into a single file (in the order indicated). For example:

```
cat host.cer imd.cer root.cer > cert-chain.cer
```

4. Combine the private key and certificate in the `jetty.pkcs12` file using the following command:

```
openssl pkcs12 -export -inkey jettyPrivate.key -in cert-chain.cer -out  
jetty.pkcs12 -name jetty
```

5. Enter the password that you provided when creating the CSR (default: `megha.jeos`).
6. Stop the `crond` service using the command:

```
service crond stop
```

7. Stop all the running services using the following command:

```
/usr/local/megha/bin/stop-all-services.sh
```

8. Verify that the `megha` and `crond` services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

9. Create a backup of the existing keystore file using the following command:

```
mv /usr/local/megha/jetty/etc/keystore /usr/local/megha/jetty/etc/keystore-orig
```

10. Create a backup of an existing `userKeystoreConfig` file using the following command:

```
cp /usr/local/megha/jetty/etc/userKeystoreConfig.xml /usr/local/megha/jetty/etc/  
userKeystoreConfig-orig.xml
```

11. Import the `pkcs12` file (using `keytool`) using the following command:

```
keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12 -  
destkeystore keystore -deststoretype PKCS12
```

12. Enter the password that you provided when creating the CSR (default: `megha.jeos`).



Note: If you provided a password of your choice when creating the CSR, make sure you change the following fields in the `/usr/local/megha/jetty/etc/userKeystoreConfig.xml` file.

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

If the password includes the following special characters, you must replace them as indicated when editing these fields:

- Replace ' ' with '"'
- Replace ' ' with '''
- Replace ' < ' with '<'
- Replace ' > ' with '>'
- Replace ' & ' with '&'

For example:

- Replace `abc"123` with `abc"123`
- Replace `abc '123` with `abc'123`
- Replace `abc&"123` with `abc&"123`

(Optional): If you want an encrypted password for security purpose, you can convert the password into OBF format using the following command and provide the converted password in the `userKeystoreConfig.xml` file:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty Version>.jar
org.eclipse.jetty.util.security.Password
"password_provided_when_creating_CSR"
```

For example:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-12.0.4.jar
org.eclipse.jetty.util.security.Password "abc&123"
```

If the password contains " quotation mark, provide the password within ' ' quotation marks in the above command. For example: `'abc"123'`

13. Change the ownership and permission of the keystore file:

```
chown megha:megha /usr/local/megha/jetty/etc/keystore
```

```
chmod og-rwx /usr/local/megha/jetty/etc/keystore
```

14. Start the megha service using the following command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

15. Start the crond service using the following command:

```
service crond start
```

16. (Optional) Remove the `certreq.csr`, `cert-chain.cer`, and `jetty.pkcs12` files if you will not need them in the future:

```
rm /tmp/certreq.csr
rm /usr/local/megha/jetty/etc/cert-chain.cer
rm /usr/local/megha/jetty/etc/jetty.pkcs12
```

Configuring a self-signed SSL certificate (Analyzer detail view server)

You can configure a self-signed SSL certificate for browser sessions for test purpose by creating a private key, a certificate signing request (CSR), and applying the server certificate.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like `putty`) as a root user.
2. Create a temporary directory and open it:

```
mkdir /tmp/SelfSignedCertificate
```

```
cd /tmp/SelfSignedCertificate
```

3. Create a private key using one of the following algorithms:

RSA:

```
openssl genrsa -out jettyPrivate.key
```

ECDSA:

```
openssl ecparam -out jettyPrivate.key -name prime256v1 -genkey
```

4. Create a certificate signing request (CSR):

```
openssl req -new -key jettyPrivate.key -out certreq.csr
```

Follow the instructions displayed on the console to enter the details for your certificate request (including the CSR password). For the common name, make sure that you enter the fully qualified host name.

5. Generate a self-signed certificate from the CSR:

```
openssl x509 -req -days 365 -in certreq.csr -signkey jettyPrivate.key -out certreq.cer
```

6. Combine the private key and certificate in the `jetty.pkcs12` file as shown in the following example:

```
openssl pkcs12 -export -inkey jettyPrivate.key -in certreq.cer -out jetty.pkcs12  
-name jetty
```

Enter the export password. (The default is `megha.jeos`)



Note: If you do not use the default password, you must edit the `userKeystoreConfig.xml` file as follows:

- a. Open the `userKeystoreConfig.xml` file:

```
vi /usr/local/megha/jetty/etc/userKeystoreConfig.xml
```

- b. Update the following fields and save the file:

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

If the password includes the following special characters, you must replace them as indicated when editing these fields:

- Replace ' ' with '"'
- Replace ' ' with '''
- Replace ' < ' with '<'
- Replace ' > ' with '>'
- Replace ' & ' with '&'

For example:

- Replace `abc"123` with `abc"123`
- Replace `abc '123` with `abc'123`
- Replace `abc&"123` with `abc& "123`

(Optional): If you want an encrypted password for security purpose, you can convert the password into OBF format using the following command and provide the converted password in the `userKeystoreConfig.xml` file:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty
Version>.jar org.eclipse.jetty.util.security.Password
"password_provided_when_creating_CSR"
```

For example:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-12.0.4.jar
org.eclipse.jetty.util.security.Password "abc&123"
```

If the password contains " quotation mark, provide the password within ' ' quotation marks in the above command. For example: `'abc"123'`

7. Stop the crond service:

```
service crond stop
```

8. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

9. Create a backup of the existing keystore file using the following command:

```
mv /usr/local/megha/jetty/etc/keystore /usr/local/megha/jetty/etc/keystore-orig
```

10. Import `jetty.pkcs12` into the keystore to import the self-signed certificate using the following command:

```
keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12 -  
destkeystore /usr/local/megha/jetty/etc/keystore -deststoretype PKCS12
```

Enter the destination and source keystore passwords you used in step 6.

11. Change the ownership and permission of the keystore file:

```
chown megha:megha /usr/local/megha/jetty/etc/keystore
```

```
chmod og-rwx /usr/local/megha/jetty/etc/keystore
```

12. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

13. Start the crond service:

```
service crond start
```

14. (Optional) Remove the `SelfSignedCertificate` directory if you will not need it in the future:

```
cd /tmp
```

```
rm -rf /tmp/SelfSignedCertificate
```

Exporting a self-signed certificate for the Analyzer detail view server

Use the `keytool` command to export self-signed certificates.

Procedure

1. Run the following command to export the certificate for the Analyzer detail view server:

```
keytool -export -keystore /usr/local/megha/jetty/etc/keystore -alias alias-name -  
file certificate-file-name
```

**Note:**

- For the *alias-name*, specify `jetty` to export the default self-signed certificate.
- For *certificate-file-name*, specify the absolute path to the export destination of the self-signed certificate.

For example:

```
keytool -export -keystore /usr/local/megha/jetty/etc/keystore -
alias jetty -file /root/test/Certificate
```

Checking the expiration dates of certificates for Analyzer detail view server

Check the expiration dates of the server certificates and Certificate Authority certificates for Analyzer detail view server.

Procedure

1. Run the following command to check the expiration date:

```
keytool -list -v -keystore /usr/local/megha/jetty/etc/keystore
```



Note: You must use the keystore password of the Analyzer detail view server.

Sample output:

```
Valid from: Thu Nov 27 04:43:53 EST 2014 until: Tue Nov 26
04:43:53 EST 2024
```

Changing the SSL or HTTPS port number of the Analyzer detail view server

To change the port number for SSL or HTTPS communication, you must change the port numbers specified in the definition file, and then open the new port in the firewall settings.

Before you begin



Note: If you do not want to stop the `crond` service, you can stop specific processes of the Analyzer detail view server and Analyzer probe server by using the `crontab -e` command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 153\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 154\)](#)

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like `putty`) as a root user.

2. Stop the crond service and verify the status with these commands:

```
service crond stop
service crond status
```

3. Stop all the services and verify the megha service status with these commands:

```
/usr/local/megha/bin/stop-all-services.sh
/usr/local/megha/bin/megha-jetty.sh status
```

4. Make a backup of the `server.ini` file:

```
cp /usr/local/megha/jetty/start.d/server.ini /usr/local/megha/jetty/start.d/
org_server.ini.backup
```

5. Change the port number in the `/usr/local/megha/jetty/start.d/server.ini` file. For example:

```
jetty.httpConfig.securePort=9443

jetty.ssl.port=9443
```

6. Start the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh start
/usr/local/megha/bin/megha-jetty.sh status
```

7. Start the crond service and verify the status with these commands:

```
service crond start
service crond status
```

8. After changing the port number, make sure you change the firewall settings accordingly.

Next steps

If you are using the Common Services, make sure that you also update the port number using the `setupcommonservice` command to update the port number in Common Services.

Changing the port for On-demand real time monitoring of Hitachi Enterprise Storage

By default, port 24262 is used for communication between the Analyzer detail view server and RAID Agent server for On-demand real time monitoring. To change this default, you must configure properties in the Analyzer detail view server.

Before you begin

If the Analyzer detail view server is receiving data from multiple RAID Agent servers and you want to configure a separate port for each server, you need to know the RAID Agent server

IP addresses available in the Analyzer detail view server. To identify the IP addresses, do the following:

1. Log on to the Analyzer detail view UI.
2. From the left pane, click **Reports > Build**.
The **Build** window opens.
3. Click **Create Using MQL**.
4. Enter the following query in the **MQL** box using the following format:

```
raidStorage[=serialNumber rx serialNumber]/raidAgentInstance[=raHost rx .*]
```

For example:

```
raidStorage[=serialNumber rx 421358]/raidAgentInstance[=raHost rx .*]
```

5. Click **View Result**.
The **View Result** window opens.
6. In the **View Result** window, click the desired resource in the **Resource** column.
The RAID Agent server IP address is displayed in the **RAID Agent Host** column.
7. Copy the IP address.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Stop the crond service and verify the status with these commands:

```
service crond stop
service crond status
```

3. Stop the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh stop
/usr/local/megha/bin/megha-jetty.sh status
```

4. Make a backup of the **custom.properties** file:

```
cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
custom_orig.properties
```

5. Edit the **custom.properties** file.

```
vi /usr/local/megha/conf/custom.properties
```

6. Change the port as follows:

- If you want to use one port to communicate with all RAID Agent servers available in Analyzer detail view server, add the following property:

```
default.raidAgent.port=port_Number
```

For example:

```
default.raidAgent.port=25663
```

- If you want to use a different port to communicate with each RAID Agent server, add a separate entry for each server as follows:

```
RAID_Agent_Server_IP_address.raidAgent.port=Port_Number
```

For example:

```
192.168.100.52.raidAgent.port=80
192.168.20.27.raidAgent.port=89
```

7. Save the `custom.properties` file.

8. Start the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh start
/usr/local/megha/bin/megha-jetty.sh status
```

9. Start the crond service and verify the status with these commands:

```
service crond start
service crond status
```

Enabling TLS certificate verification for the On-demand real time monitoring

The TLS certificate verification enables secure communication between the Analyzer detail view server and the RAID Agent server (usually, the host on which the Analyzer probe server is installed) for On-demand real time monitoring.

Before you begin

- Obtain a valid TLS certificate (for example, `server.crt` file) from the RAID Agent server and save it in the `/tmp` directory on the Analyzer detail view server.

TLS certificate verification is a global setting. If there are multiple RAID Agent servers available in the Analyzer detail view server, make sure you obtain the TLS certificates for all the RAID Agent servers.

- Identify and note the Java keystore path on the Analyzer detail view server machine.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like putty) as a root user.
2. Stop the crond service using the command:

```
service crond stop
```

3. Stop the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

4. Make a backup of the `custom.properties` file:

```
cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/  
custom_orig.properties
```

5. Edit the `custom.properties` file.

```
vi /usr/local/megha/conf/custom.properties
```

6. Add a new entry in the property file:

```
realtimemonitoring.verify.tls.certificate=true
```

7. Save the `custom.properties` file.
8. Navigate to the Java keystore directory. For example:

```
/usr/lib/jvm/java-17-amazon-corretto/lib/security
```

9. If the `jssecacerts` file does not exist, create it.
10. Import the TLS certificate into the Analyzer detail view server using the `keytool` command:

```
keytool -importcert -alias Alias_name -keystore Truststore_file_path -storetype  
jks -storepass Truststore_file_password -file TLS_certificate_file_path
```



Note: You can define any unique alias name for TLS certificate.

For example:

```
keytool -importcert -alias aliasName -keystore jssecacerts -storetype jks -  
storepass changeit -file /tmp/server.crt
```

11. If there are multiple RAID Agent servers, repeat step 10 for each instance.
12. Make sure that the megha user has the read permission for the `jssecacerts` file. If not, change the permissions as in this example:

```
chmod o+r jssecacerts
```

13. Start the megha service and verify the status:

```
/usr/local/megha/bin/megha-jetty.sh start
/usr/local/megha/bin/megha-jetty.sh status
```

14. Start the crond service and verify the status:

```
service crond start
service crond status
```



Note: If you upgrade the JDK in the future, make sure that the `jssecacerts` file is copied in the upgraded JDK directory.

For example: If you upgrade JDK from v1.8.0 to v17, copy the `jssecacerts` file from `/usr/java/jdk1.8.0_291-amd64/jre/lib/security` to `/usr/lib/jvm/java-17-amazon-corretto/lib/security`.

After copying the `jssecacerts` file, make sure that megha user has read permission for the `jssecacerts` file.

Importing TLS or SSL certificate for the SMTP Server

The TLS or SSL certificate enables secure communication between the Analyzer detail view server and the SMTP Server to send alerts.

Before you begin

- Obtain a valid TLS or SSL certificate (for example, `server.crt` file) from the SMTP server and save it in the `/tmp` directory on the Analyzer detail view server.



Note: The procedure for importing TLS and SSL certificates is the same.

- Identify and note the Java keystore path on the Analyzer detail view server machine.

Procedure

- Log on to the Analyzer detail view server through an SSH client (like putty) as a root user.
- Stop the crond service using the command:

```
service crond stop
```

- Stop the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

- Navigate to the Java keystore directory. For example:

```
cd /usr/java/jdk1.8.0_291-amd64/jre/lib/security
```

5. If the `jssecacerts` file does not exist, create it.
6. Import the TLS or SSL certificate into the Analyzer detail view server using the **keytool** command:

```
keytool -importcert -alias Alias_name -keystore Truststore_file_path -storetype  
jks -file TLS_OR_SSL_certificate_file_path
```



Note: You can define any unique alias name for TLS or SSL certificate.

For example:

```
keytool -importcert -alias aliasName -keystore jssecacerts -storetype jks -  
file /tmp/server.crt
```



Note: Enter the truststore password when prompted.

7. Make sure that the megha user has the read permission for the `jssecacerts` file. If not, change the permissions as in this example:

```
chmod o+r jssecacerts
```

8. Start the megha service and verify the status:

```
/usr/local/megha/bin/megha-jetty.sh start  
/usr/local/megha/bin/megha-jetty.sh status
```

9. Start the crond service and verify the status:

```
service crond start  
service crond status
```



Note: If you upgrade the JDK in the future, make sure that the `jssecacerts` file is copied in the upgraded JDK directory.

For example: If you upgrade JDK from v1.7.0 to v1.8.0, copy the `jssecacerts` file from `/usr/java/jdk1.7.0_291-amd64/jre/lib/security` to `/usr/java/jdk1.8.0_251-amd64/jre/lib/security`.

After copying the `jssecacerts` file, make sure that megha user has read permission for the `jssecacerts` file.

Stopping the Analyzer detail view server or Analyzer probe server services

Stop the Analyzer detail view server or Analyzer probe server services by editing `crontab`.

Before you begin

Log on to the Analyzer detail view server or Analyzer probe server as the megha user.

Procedure

1. Run the `crontab -e` command.
2. At the beginning of each line add a hash mark (#) to comment out a line as shown in this example:

```
# */5 * * * * F=/usr/local/megha/cron.5min; test -f $F && sudo $F
# */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (sudo $F >> /usr/
local/megha/logs/sys/`date +%Y%m%d`.log; chown -R megha:megha /usr/local/
megha/logs/sys)
```

3. Stop all services using the command:

```
sudo /usr/local/megha/bin/stop-all-services.sh
```

4. Confirm the megha service has stopped:

```
/usr/local/megha/bin/megha-jetty.sh status
```

Starting the Analyzer detail view server or Analyzer probe server services

Start the Analyzer detail view server or Analyzer probe server services by editing `crontab`.

Before you begin

- Make sure that the following disk space is available:
 - Analyzer probe server:
 - Installation directory: More than 5 GB or 5% available of the total disk space
 - /etc: 100 MB (Available)



Note: The Analyzer probe server retrieves the partition details where the directories are mounted and checks the free disk space. Make sure that the required disk space is available on partition in case multiple directories are mounted on it.

- Analyzer detail view server:
 - Installation directory: More than 5 GB or 5% of the total disk space
- Log on to the Analyzer detail view server or Analyzer probe server as the megha user.

Procedure

1. Run the `crontab -e` command.

2. Delete the hash marks (#) from the beginning of each line as shown in this example:

```
* /5 * * * * F=/usr/local/megha/cron.5min; test -f $F && sudo $F
* /5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (sudo $F >> /usr/
local/megha/logs/sys/`date +%Y%m%d`.log; chown -R megha:megha /usr/local/
megha/logs/sys)
```

3. Start the megha service using the command:

```
sudo /usr/local/megha/bin/megha-jetty.sh start
```

4. Confirm the megha service has started:

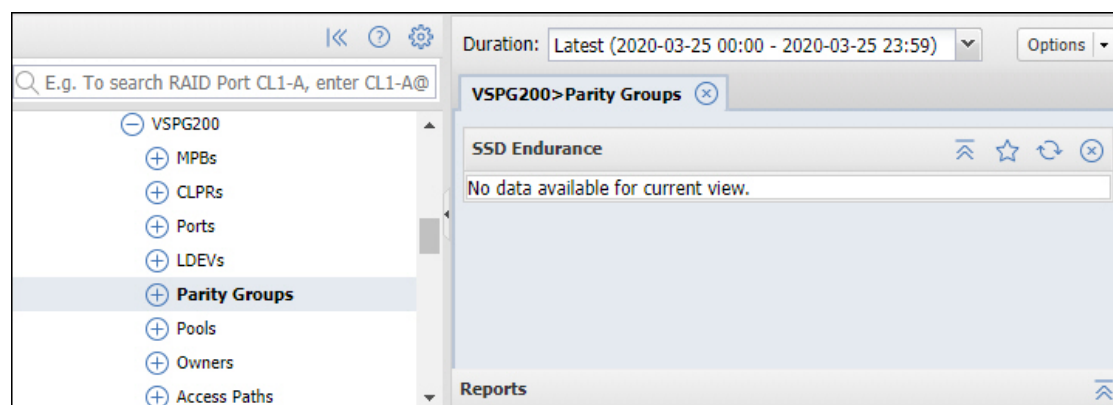
```
/usr/local/megha/bin/megha-jetty.sh status
```

Chapter 8: Troubleshooting

SSD Endurance report does not show any data

SSD endurance is the total amount of data that an SSD is guaranteed to write under warranty. The SSD Endurance report lists SSD drives with an endurance usage exceeding 50%. It helps you to take corrective actions to avoid data loss. (This report is displayed for a certain Hitachi Storage system models on the Parity Group group level node.)

Sometimes the SSD Endurance report includes the message `No data available for current view`. Verify the storage systems models, endurance value, and drive type as described in the following sections.



Storage system models

The SSD Endurance report is supported only for the following storage system models:

VSP E990, VSP F350, VSP F370, VSP F700, VSP F900, VSP G350, VSP G370, VSP G700, VSP G900, VSP 5000 series AFA, and VSP 5000 series hybrid.

Verify that you are viewing the report for supported storage system. If so, verify the report criteria in the next section. If not, the Analyzer detail view is showing the message as expected.

Endurance value and drive type

Verify if used endurance exceeds 50% and the drive type is SSD.

Procedure

1. In the Analyzer detail view left pane, select **Reports > Build**. The **Build** window opens.

2. Click **Create Using MQL**.
3. Enter the following query in the **Enter MQL** box:

```
raidDrive[=usedEndurance rx .*]
```

4. Click **View Report**.
The **View Result** window opens.
5. Verify whether the used endurance exceeds 50% for any of the drive and drive type is SSD:
 - If the drive type is SSD, but used endurance is less than 50%, the Analyzer detail view is showing the proper status.
 - If the drive type is SSD and used endurance is more than 50%, the Analyzer detail view is not showing the proper status. Contact Customer Support for further investigation.

Real-time data import status is red on the Analyzer detail view UI

If the Analyzer detail view server does not receive real-time data within a default threshold, the status is shown as red in the Analyzer detail view **Status** window. (This can be caused by such issues as network latency.) To resolve this problem, one solution can be to increase the default threshold of 6 minutes.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Stop the crond service and verify the status with these commands:

```
service crond stop  
service crond status
```

3. Stop all the services and verify the megha service status with these commands:

```
/usr/local/megha/bin/stop-all-services.sh  
/usr/local/megha/bin/megha-jetty.sh status
```

4. Create a backup of the `custom.properties` file using the following command:

```
cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/  
backup_custom_backup.properties
```

5. Edit the `custom.properties` file.

```
vi /usr/local/megha/conf/custom.properties
```

6. Add the following property with threshold value in minutes:

```
realtime.probe.importer.perf.threshold=threshold_in_minutes
```

For example:

```
realtime.probe.importer.perf.threshold=20
```

7. Save the file and exit.
8. Start the megha service and verify the status with these commands:

```
/usr/local/megha/bin/megha-jetty.sh start  
/usr/local/megha/bin/megha-jetty.sh status
```

9. Start the crond service and verify the status with these commands:

```
service crond start  
service crond status
```

Troubleshooting the Analyzer detail view server or Analyzer probe server

When you receive an email alert from AAM, you should follow these procedures to connect to the HDEBBUG shell and troubleshoot the issue.

You can also disable or enable the statics collection of System Diagnostics using the procedures in this section.

Connecting to the HDEBBUG shell

Use the HDEBBUG shell to troubleshoot Analyzer detail view server or Analyzer probe server problems.

Before you begin

The Advanced Activity Monitor must be enabled.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like putty) using the account specified in the email alert.
2. Open the HDEBBUG shell using the following command:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh
```
3. Connect as an Analyzer detail view server or Analyzer probe server user:
 - a. Run the command: `connect --u user-name`

For example: `connect --u admin`

**Note:**

- Only the Active Directory and Local type of users can connect to the HDEBBUG shell.
- Active Directory users must include the fully qualified domain name using one of the following formats:

- *FQDN\user-name*

Example: corp.company\smith

- *user-name@domain-name*

Example: smith@corp.company

- b. Enter the password.



Note: The HDEBBUG shell saves the login information, so you will not need to enter the credentials next time you log in.

To disconnect from the HDEBBUG shell, type `disconnect` and then `exit`.

Downloading the debug data file

If you are unable to resolve a Ops Center Analyzer detail view problem reported in an AAM alert, you can download the debug data file and send it to Customer Support. (The debug data file location is provided in the alert.)

Procedure

1. Connect to the Analyzer detail view server or Analyzer probe server through an FTP client (like WinSCP) using the following credentials:
 - User: megha
 - Password: User password
 - Port: 22
2. Go to the location specified in the AAM alert and download the debug data file.
3. Contact Customer Support by following the following link and provide the data file: https://support.hitachivantara.com/en_us/contact-us.html

Diagnosing a probe using the HDEBBUG shell

If a problem occurs when adding or using a probe in the Analyzer probe server, you can diagnose the problem using the interactive HDEBBUG shell. The following probes are supported:

- Hitachi Enterprise Storage
- VMware
- VMAX

Diagnosing a problem when adding a probe

If a failure occurs while attempting to add a probe, follow these steps.

Procedure

1. Connect to the HDEBBUG shell as the `megha` or `root` user.
2. Run the following command:
`diagnoseProbe --i`
3. Choose the probe type and enter the required details. For example, if you choose 2 (HitachiEnterpriseStorage probe), provide the connection type, RAID agent IP address, host name, port, and so on.
4. HDEBBUG validates your entries and displays the diagnosis. In the following example, the diagnosis suggests that the probe is unable to collect data because the latest data is unavailable from the RAID Agent (possibly because the RAID Agent instance service is not running). You can try to resolve this issue by starting the RAID Agent instance service.

```
Verifying Telnet Connection on (192.168.100.73:24221)...
Result: Success

Verifying PD Record...
INPUT_RECORD_TYPE,DATETIME,GMT_ADJUST,RECORD_TIME,COLLECTION_TIME,INTERVAL,DKC_S
ERIAL_NUMBER,UNIT_ID,VENDOR_ID,DKC_NAME,DKC_STATUS,CACHE_MEMORY_CAPACITY,CACHE_M
EMORY_INSTALLED_SIZE,MONITORED_SLPR_NUMBER
string(8),time_t,long,time_t,time_t,ulong,string(32),unsigned char,string(64),s
tring(64),unsigned char,ulong,ulong,string(8)

HDCA fails to add the probe due to unavailability of latest data with RA. For fu
rther troubleshooting, please refer to Cumulus Systems Knowledge Base(KB) portal
Result: Failure

Hitachi Enterprise Storage Summary Result
Checkpoints Run: 2
Checkpoints Failed: 1
Checkpoints Passed: 1

Done!!!
```

Diagnosing a problem after adding a probe

If a failure occurs after you have successfully added a probe, follow these steps.

Procedure

1. Connect to the HDEBBUG shell as the `megha` or `root` user.
2. Run the `diagnoseProbe` command and specify the probe instance (number).
For example: `diagnoseProbe --probeName "421358"`
3. HDEBBUG displays the diagnosis on the CLI. The following example shows that data collection has stopped because the Analyzer probe server is unable to connect to the RAID Agent server on port 24221, possibly because the RAID Agent services (REST Application Service and REST Web Service) are not running. You can try to resolve this issue by starting these services.

```

admin@localhost>diagnoseProbe --probeName "421358"

Verifying Telnet Connection on (192.168.100.73:24221)...
Result: Failure

Verifying PD Record...
INPUT_RECORD_TYPE,DATETIME,GMT_ADJUST,RECORD_TIME,COLLECTION_TIME,INTERVAL,DKC_S
ERIAL_NUMBER,UNIT_ID,VENDOR_ID,DKC_NAME,DKC_STATUS,CACHE_MEMORY_CAPACITY,CACHE_M
EMORY_INSTALLED_SIZE,MONITORED_SLPR_NUMBER
string(8),time_t,long,time_t,time_t,ulong,string(32),unsigned char,string(64),s
tring(64),unsigned char,ulong,ulong,string(8)

HDCA fails to add the probe due to unavailability of latest data with RA. For fu
rther troubleshooting, please refer to Cumulus Systems Knowledge Base(KB) portal
Result: Failure

____Hitachi Enterprise Storage Summary Result____
Checkpoints Run: 2
Checkpoints Failed: 2
Checkpoints Passed: 0

Done!!!
Verifying Telnet Connection on (192.168.20.27:2443)...
Result : Failure

____Hitachi Device Manger Summary Result____
Checkpoints Run: 1
Checkpoints Failed: 1
Checkpoints Passed: 0

Done!!!

```

Editing Analyzer detail view AAM alerts

You can change the default alert thresholds or disable an alert if you no longer want to receive it.

Procedure

1. Connect to the HDEBUG shell as the `megha` or `root` user.
2. Run the following command:

```
editRule
```

```

admin@localhost>editRule
RuleID Rule Severity Rule
1 Critical Syslogd process is not running.
2 Warning Disk is %value full.
3 Critical Disk utilization exceeds 90%; Read only mode.
4 Fatal Disk is 95% full; Shutting down
5 Critical File System is read-only.
6 Warning High CPU usage.
7 Warning High Open File Count.
8 Critical crond process is not running.
9 Critical Web Server unresponsive.
10 Critical Jetty service is not running.

```

3. To edit the rule, type `y` and then press **Enter**.
4. Enter the alert ID (rule) that you want to edit and then press **Enter**.

5. Do the following:
 - To edit the threshold, provide the threshold value and then press **Enter**. (Skip editing the threshold by pressing **Enter**.)
 - To disable an alert, enter `Disabled` and then press **Enter**.
6. If you are prompted for additional inputs, ignore them and press **Enter**.
A message is displayed confirming that your edits are saved. The settings will go into effect when the next alert cycle begins.

Enabling the Advanced Activity Monitor

By default, AAM is enabled on both the Ops Center Analyzer detail view and Analyzer probe servers. If you have disabled it, you can enable it using this procedure. When enabled, cron will automatically start AAM each time the server is booted.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like putty) using the following credentials:
 - User: `megha`
 - Password: Enter the megha user password.
2. Run the following command:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh setAAMConfig --key aam.enabled --value true
```

The cron process will automatically start AAM within five minutes. To start AAM immediately, use the following command:

3. Start AAM, using the following command:

```
/usr/local/megha/dbgUtils/bin/manage-aam.sh start
```

Disabling the Advanced Activity Monitor

By default, AAM is enabled for the Analyzer detail view server or Analyzer probe server. You can disable it using this procedure.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like putty) using the following credentials:
 - User: `megha`
 - Password: Enter the megha user password.

2. Run the following commands:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh setAAMConfig --key  
aam.enabled --value false  
  
/usr/local/megha/dbgUtils/bin/manage-aam.sh stop
```

Disabling statistics collection for Analyzer detail view System Diagnostics

By default, System Diagnostics is enabled on the Analyzer detail view server and Analyzer probe server for collection of operating statistics. You can disable the statistics collection using this procedure.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like putty) using the following credentials:
 - User: megha
 - Password: Enter the megha user password.
2. Run the following commands:
 - ```
/usr/local/megha/dbgUtils/bin/hdebug.sh
setSystemDiagnosticsConfig --key sds.enabled --value false
```
  - ```
/usr/local/megha/dbgUtils/bin/manage-sds.sh stop
```

The statistics collection is stopped. But you can still access System Diagnostics by launching it from the Analyzer detail view server UI to view historical data in reports.

Enabling statistics collection for Analyzer detail view System Diagnostics

By default, System Diagnostics is enabled on the Analyzer detail view server and Analyzer probe server for collection of operating statistics. If you have disabled collection, you can enable it using this procedure.



Note: The System Diagnostics data is not collected for the Analyzer probe server if the HTTPS protocol is used to upload data from the Analyzer probe server to the Analyzer detail view server.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like putty) using the following credentials:
 - User: megha
 - Password: Enter the megha user password.

2. Run the following commands:

- `/usr/local/megha/dbgUtils/bin/hdebug.sh
setSystemDiagnosticsConfig --key sds.enabled --value true`
- `/usr/local/megha/dbgUtils/bin/manage-sds.sh start`

The operating statistics collection is started.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA



HitachiVantara.com/contact