CENTERITY

Centerity Monitor Version 5.05:
User Guide

March 2020

End-User License Agreement (EULA)

This guide and the use of Centerity software is subject to Centerity's End-User License Agreement (EULA). A copy of Centerity's EULA can be found here.

Table of Contents

1. About This Guide **6**
1.1 Before You Begin 6
1.2 Audience 6
1.3 Centerity Monitor Admin Guide 6
2. Technical Support **7**
3. Overview **8**
3.1 Centerity Monitor Enterprise Edition - Introduction 8
3.2 Centerity Monitor Main Features 8
3.3 Start Using Centerity Monitor 9
4. General Overview **10**
4.1 Dashboard 10
4.2 Settings 11
4.3 Event Console 11
4.4 Host and Metrics 14
4.4.1 Host States 14
4.4.2 Metric States 14
5. Host-Group and Host Management **15**
5.1 Overview 15
5.2 Host Group Management 15
5.3 Host Management 18
6. Metrics **23**
7. Business Services **27**
7.1 Overview 27
7.2 Detailed BSM information 27
8. Root Cause Analysis **30**
9. Status Map **31**
9.1 Overview 31
9.2 Visual Layouts - Hypermap 31
9.3 Topology Map 32

9.4 Maps Dashboard 32
9.5 Visual Layouts – Maps Views 34
10. Reports 35
10.1 Reports option 35
10.1.1 SLA Report 35
10.1.2 Event Level Report 38
10.1.3 History Report 40
10.1.4 Inventory Report 42
10.1.5 Inventory Summary Report 44
10.1.6 SNMP Traps Report 46
10.1.7 Syslog Report 47
10.1.8 Summary Report 48
10.1.9 Charts Report 49
10.1.10 Trends Report 51
10.1.11 Uptime Report 53
10.1.12 Usage Summary Report 55
10.1.13 Utilization Report 58
10.2 Creating a New Report Template 59
Appendix A. Traffic Analyzer 61
A.1 Using the Traffic Dashboard 61
A.1.1 Viewing the Traffic Dashboard 64
A.1.2 Modifying the Recent Active Flows Time Frame 64
A.1.3 Managing Preference Tools 65
A.1.4 Creating a New Traffic Dashboard 66
A.1.5 Switching Traffic Dashboards 67
A.1.6 Deleting a Traffic Dashboard 67
A.2 Viewing Recent Active Flows 68
A.2.1 Viewing Recent Active Flows 71
A.2.2 Managing Your Recent Active Flows View 71
A.3 Viewing Alerts 72
A.3.1 Viewing Alerts 73
A.3.2 Managing Your Alerts View 73

A.4 Generating Reports 74
A.4.1 Summary Report 75
A.4.2 Search Report 78
A.4.3 Saved Reports 80

1. About This Guide

This Centerity Monitor User Guide describes how to operate the Centerity Monitor system as a user. For administrative operation use the Centerity Admin Guide.

1.1 Before You Begin

This manual assumes that you have installed the Centerity Monitor software and logged into the web console as described in the Centerity Monitor Installation guide. For installation guide please click here.

1.2 Audience

This User-Guide is intended for NOC / system administrators who are responsible for the daily use of the Centerity system.

2. Technical Support

For technical support, contact Centerity at:

Email (EMEA): support@centerity.com

Email (US): support_us@centerity.com

Phone (EMEA): +972 (0)9-765-8080

Phone (U.S.): +1 (339) 225-6064 (EXT: 1005)

Or contact your local Centerity partner.

Check our website (http://www.centerity .com) for additional information and most updated technical information.
Under the support section you can find information including how-to documents, solution packs, certified plugins and more.

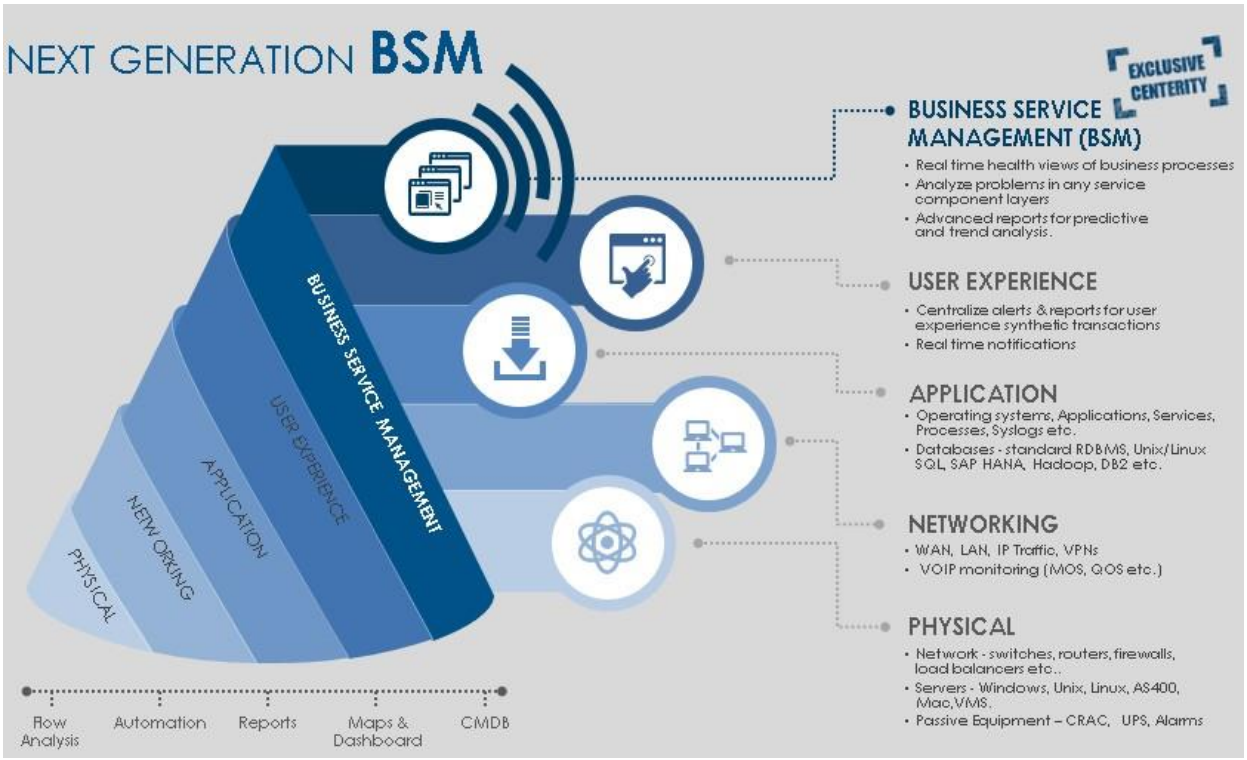
With any support contact please provide the following information:

- License version
- Server's configuration and operating system, including any OS patches that have been applied.
- Detailed description of the requires support assistance
- Relevant attachments such as error messages, memory dumps, compiler listings, and error logs

3. Overview

3.1 Centerity Monitor - Introduction

Centerity Monitor is an enterprise class all-in-one IT and Business service management (BSM) monitoring platform. Centerity provides in depth monitoring capabilities for a wide range of technologies including Servers, Networks, DB, Applications, passive-equipment, Clouds, SAAS and much more while simplifying all aspects of network and IT management as well as information flow, and enhanced business performance.



3.2 Centerity Monitor Main Features

- Fast and easy deployment across large heterogenic networks.
- Multi-Tenant - Centerity enable multi-tenant management. Ideal for MSP's and organizations with multiple entities and several stand-alone networks.
- All-In-One Unified and Comprehensive monitoring platform - a single Glass Pane for all essential network information.
- Widest range of "out of the box" monitoring solution packs.
- Advanced Business Services Management (BSM) - In addition to the infrastructure monitoring features, Centerity Monitor provides the most advanced tools to measure and analyze business services SLA and user experience, monitoring.

- Most Advanced Features and Module – all included!
  - Assets management
  - Real-Time Layouts (unique feature for Centerity!)
  - Real-time Hyper-Maps
  - VMware Topology maps
  - User-Experience monitoring
  - Ticketing management including escalations
  - Repots Center
- Flexibility - In addition of hundreds of predefined best-practices monitoring templates and solution packs for most Data-Center technologies, Centerity Monitor provides an easy way to customize proprietary monitoring plug-ins within very short time and vendor independency.

3.3 Start Using Centerity Monitor

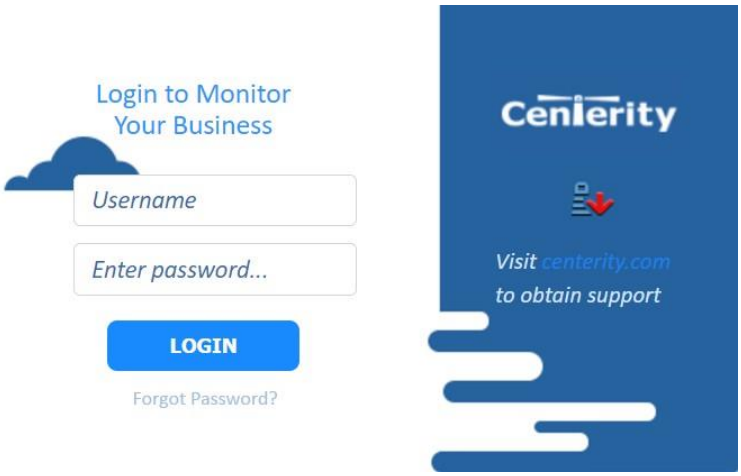
Log-in to CENTERITY MONITOR

Authentication and Permissions

Centerity Monitor installation includes 1 default read-only user:

Standard login user: **user**

Standard login password: **user**

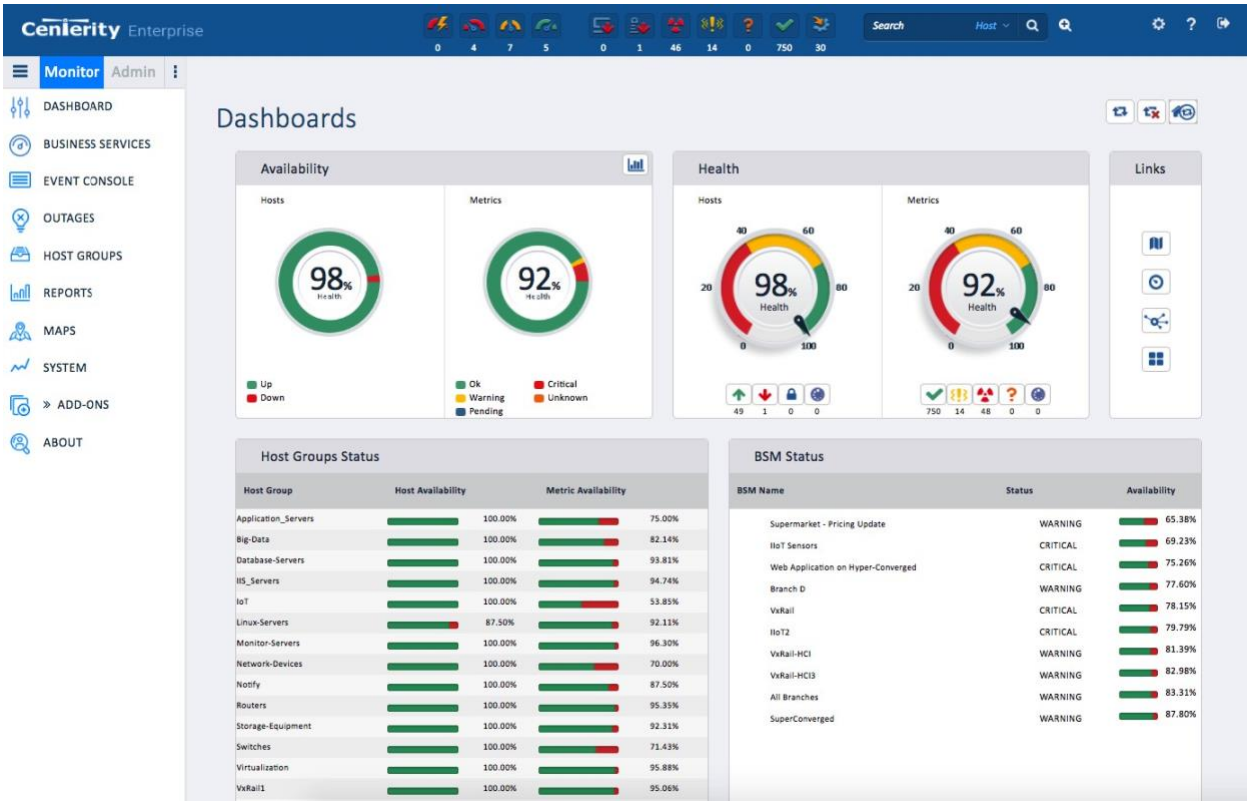


4. General Overview

4.1 Dashboard

Centerity Monitor dashboard provides a global overview of the monitored items, helping users in understanding, identifying problems and reacting immediately.

The Dashboard serves to improve the perception of IT across the enterprise. The ability to provide critical information and reporting across the business in a transparent and accountable manner will build trust and confidence. This, in turn, leads the IT department.



Centerity Monitor Dashboard

1. **Availability Charts**: The current state of host and service availability.
2. **Graph Selection** : Select a graph view for the OK / Warning / Critical / Unknown / Pending events in the last hour, Instead of the availability chart.
3. **Health**: Metric and host current health percentage compared to the entire system.
4. **Links**: Other system pages: Maps, BSMs, Hyper-Map, Event-Console.
5. Host Group Status: Availability percentage for all host group.
6. BSM Status: Availability percentage for all business views.
7. Critical Metrics Selection:

a. **View Metric Problem**: Displays most critical events in the system.

b. **Multi View**: Displays host and metric availability in host groups and service views.

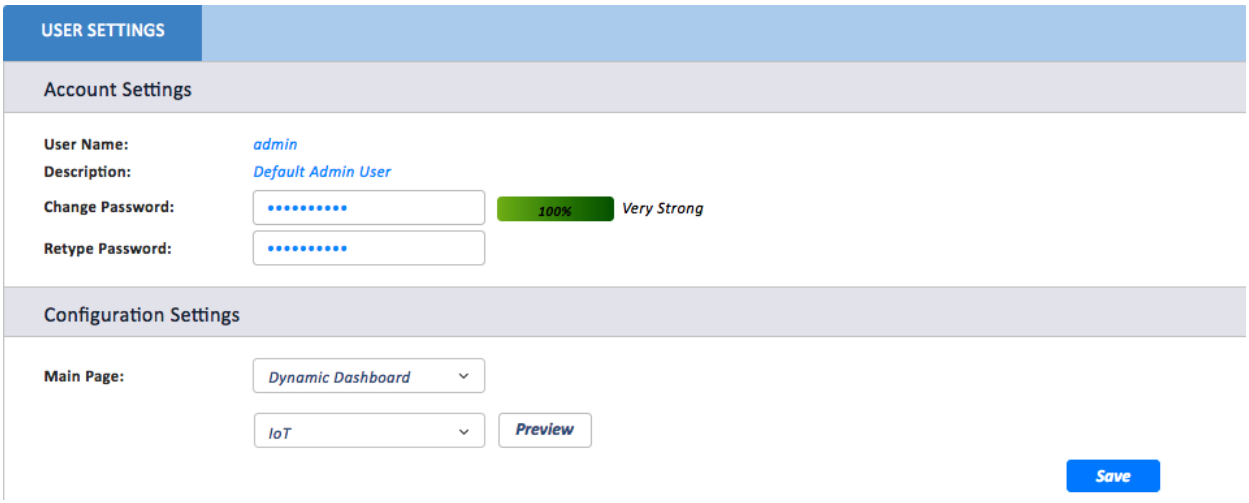
c. **Maps**: Displays selected system maps.

d. **Show Incidents**: Displays host and metric incidents, with incident summary.

4.2 Settings

The settings page is accessible from the Centerity main Dashboard:

From the setting page, any user can control its Dashboard configuration. In addition, for a local authentication system, any user can change its password.



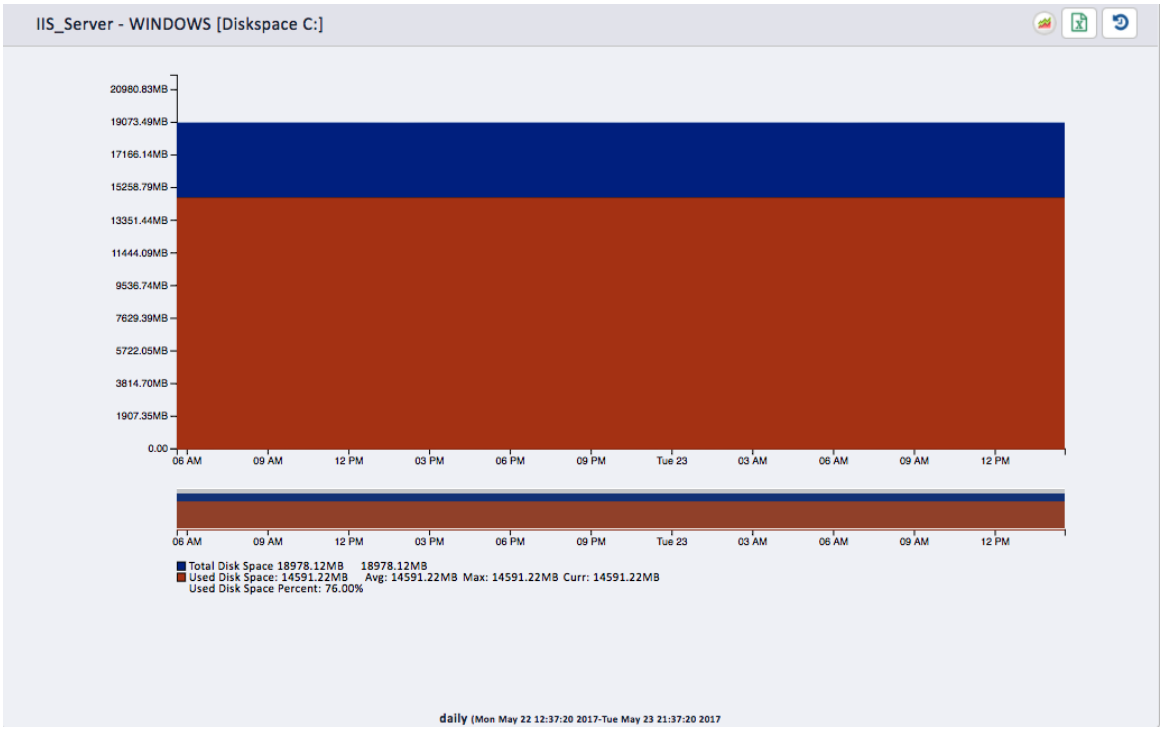
4.3 Event Console

The event console displays all current system events. All events can be sorted by host, metric, status, duration, etc.

Host	Metric	Last Check	Duration	Attempt	Information
ad.centerity.com	WINDOWS [Memory Page]	23/05/2017, 21:31:48	2w 5d 14h 46m 18s	3/3	WARNING: page file: Total: 8G - Used: 6.83G (85%) - Free: 1.16G (15%) > warning
Apache_Web_Server	APACHE [bytes per request]	23/05/2017, 21:30:49	2d 16h 49m 55s	3/3	APACHE_BYTESPERREQ WARNING - 755.361 BytesPerReq, 155.361 over warning threshold
	LINUX NO SSL [Load Avg]	23/05/2017, 21:33:07	5w 2d 14h 20m 40s	3/3	WARNING - load average: 17.63, 17.72, 17.71
CenterityRouter2.centerity.com	STATUS [GigabitEthernet0/0]	23/05/2017, 21:30:12	7h 10m 48s	3/3	CRITICAL - Interface: 2, Status: down(2) Status does not match. [crit: 1]
CenteritySW1	INTERFACE [FastEthernet0/13]	23/05/2017, 21:31:29	1w 6d 8h 56m 38s	3/3	CRITICAL. Discards in: 0 [0], Discards out: 0 [0], Errors in: 0 [68470], Errors out: 0 [0], Status: down(2), Traffic in Avg: 0 B/s (0.00%) [6470405387], Traffic out Avg: 0 B/s (0.00%) [445446357540] REASON: 22
	INTERFACE [FastEthernet0/1]	23/05/2017, 21:33:08	3h 36m 42s	3/3	CRITICAL. Discards in: 0 [0], Discards out: 0 [22], Errors in: 0 [4], Errors out: 0 [0], Status: down(2), Traffic in Avg: 0 B/s (0.00%) [47581409343], Traffic out Avg: 0 B/s (0.00%) [687570597566] REASON: 22
	INTERFACE [FastEthernet0/3]	23/05/2017, 21:33:17	1w 6d 9h 9m 48s	3/3	CRITICAL. Discards in: 0 [0], Discards out: 0 [0], Errors in: 0 [1], Errors out: 0 [0], Status: down(2), Traffic in Avg: 0 B/s (0.00%) [86941266194], Traffic out Avg: 0 B/s (0.00%) [499284674648] REASON: 22
	INTERFACE [FastEthernet0/5]	23/05/2017, 21:28:37	1d 2h 1m 21s	3/3	CRITICAL. Discards in: 0 [0], Discards out: 0 [17643], Errors in: 0 [0], Errors out: 0 [0], Status: down(2), Traffic in Avg: 0 B/s (0.00%) [2072893044], Traffic out Avg: 0 B/s (0.00%) [450441714218] REASON: 22
	INTERFACE [FastEthernet0/7]	23/05/2017, 21:29:13	1w 6d 8h 58m 58s	3/3	CRITICAL. Discards in: 0 [0], Discards out: 0 [0], Errors in: 0 [4268], Errors out: 0 [0], Status: down(2), Traffic in Avg: 0 B/s (0.00%) [2103889376], Traffic out Avg: 0 B/s (0.00%) [443560371244] REASON: 22
	INTERFACE [FastEthernet0/8]	23/05/2017, 21:29:35	1w 2d 7h 44m 35s	3/3	CRITICAL. Discards in: 0 [0], Discards out: 0 [0], Errors in: 0 [1], Errors out: 0 [0], Status: down(2), Traffic in Avg: 0 B/s (0.00%) [1591568332], Traffic out Avg: 0 B/s (0.00%) [453287156338] REASON: 22

The events table is divided into the following columns:

1. **Host**: The host name for which the event occurs.
2. **Metric**: The event metric name and its status (OK/Warning/Unknown/Critical).
3. **Last Check**: The date and time of the last executed check.
4. **Duration**: The current state duration.
5. **Attempt**: The current attempts to check the service (the limit is defined by admin).
6. Information: The metric output describing the event problem.
7. **Graphs**: Clicking on the Graph Icon will navigate to the metric daily graph:



The top row in the even console, includes filter sets. Each user has individual filter sets:

Filter By: Metric.

Metric Status: Filter by current metric status.

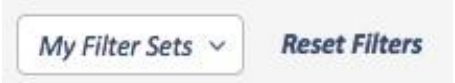
By Name / Select: Filter by metric name.

State: Filter by Downtime / Acknowledge / Checks Enabled / Notifications Enabled state.

Filter By: Host.

Host Status: Filter by current host status.

By Name / Select: Filter by host name.



My Filter Sets: Previously saved filters.

Reset Filters: View console with no filters.

4.4 Hosts and Metrics

Host: A physical or virtual server, workstation or device that resides on the network.

Metric: A KPI (Key Performance Indicator) that is monitored on a host.

4.4.1 Host States

Centerity Monitor does not execute host checks on regular basis; rather, it depends on the metrics assigned to the host being checked. If any metrics change state to critical / warning, the monitor executes a check to determine host availability.

There are four different states available for Host Checks:

- Down: The host is not responding.
- Unreachable: The host is unreachable for the system due to a network outage.
- Up: The host is reachable.
- Pending: The host has not been checked yet.

4.4.2 Metric States

Metric Checks are either executed actively on a regular basis or submitted passively by an external command interface. The metric checks are instructions for the monitor server to execute specific plug-ins and collect information regarding the metric monitored.

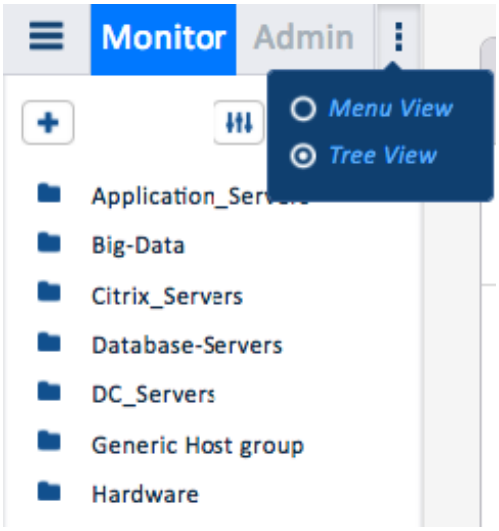
There are five different states available for Metric Checks:

- Critical: The metric check responded with a value that is within the critical level.
- Warning: The metric check responded with a value that is within the warning level.
- Unknown: The metric does not respond correctly, or it is misconfigured.
- OK: The metric check is within the ok thresholds.
- Pending: The metric has not been checked yet.

5. Host-Group and Host Management

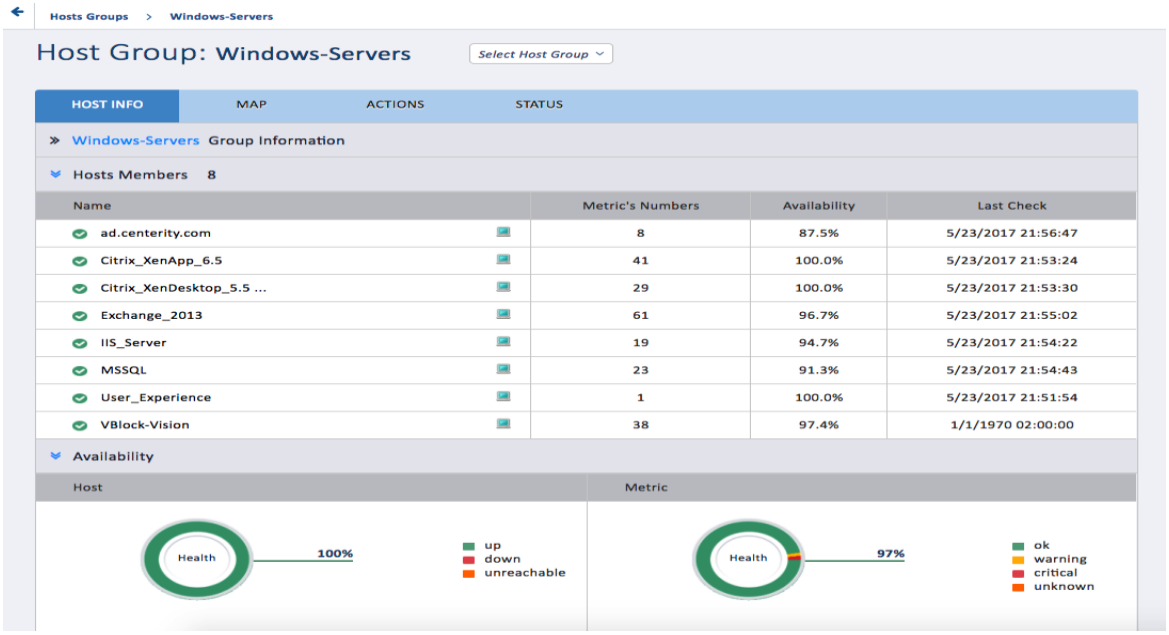
5.1 Overview

In addition to the regular monitor menu you can switch to the Tree View, which will display a Host-Group, sorted view. Host Groups are presented in the hierarchy view.



5.2 Host Group Management

By clicking any of the host-groups, the page will be redirected to the host-group page:



1. Host Info:
    a. **Group Information**: Displays any Host-Group information and comments on that host group.

b. **Host Members**: Displays host metric availability.

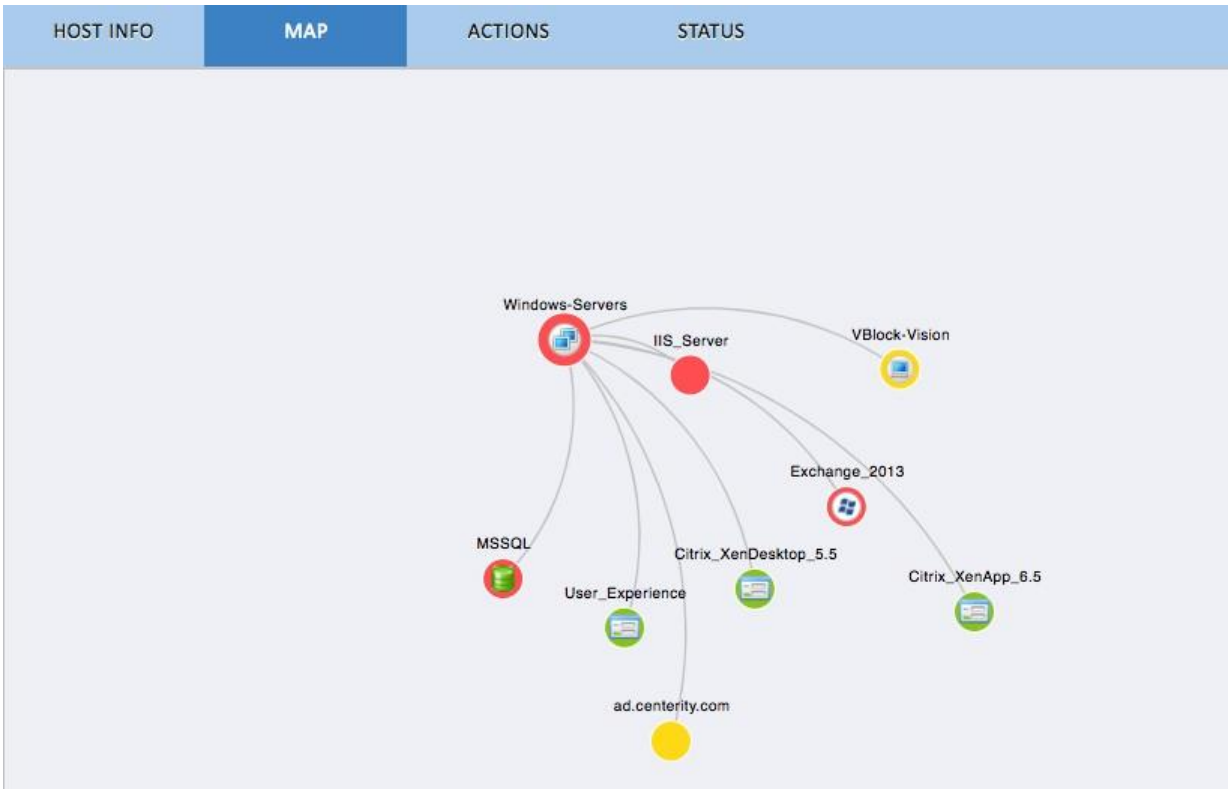
c. **Availability**: Graphically displays the hosts and metrics health under the current host group, based on the host and metric status.

d. **Sub Groups**: Displays subgroup availability under the current host group.

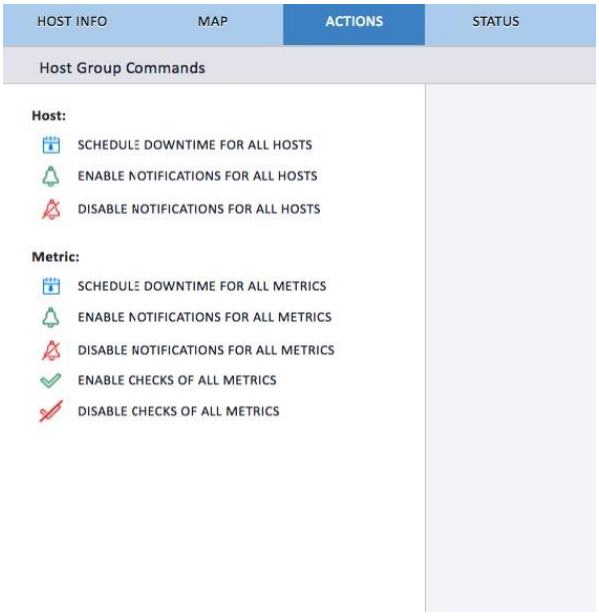
e. **Statistics**: Displays current availability and current events on host.

f. **Alerts**: Displays hosts and metrics that aren't available / scheduled to be down.

2. **Map**: Displays host-group hyper-map:



3. **Actions**:



a. **Host**:

   i. Schedule downtime for all hosts: Schedule downtime on the selected host-group.

   ii. Enable notifications for all hosts: Enable notifications for all hosts on the selected host-group.

   iii. Disable notifications for all hosts: Stop host notifications on the selected host-group.

b. **Metric**:

   i. Schedule downtime for all metrics: Schedule downtime on the all metrics in the selected host-group.

   ii. Enable notifications for all metrics: Enable notifications for all metrics on the selected host-group.

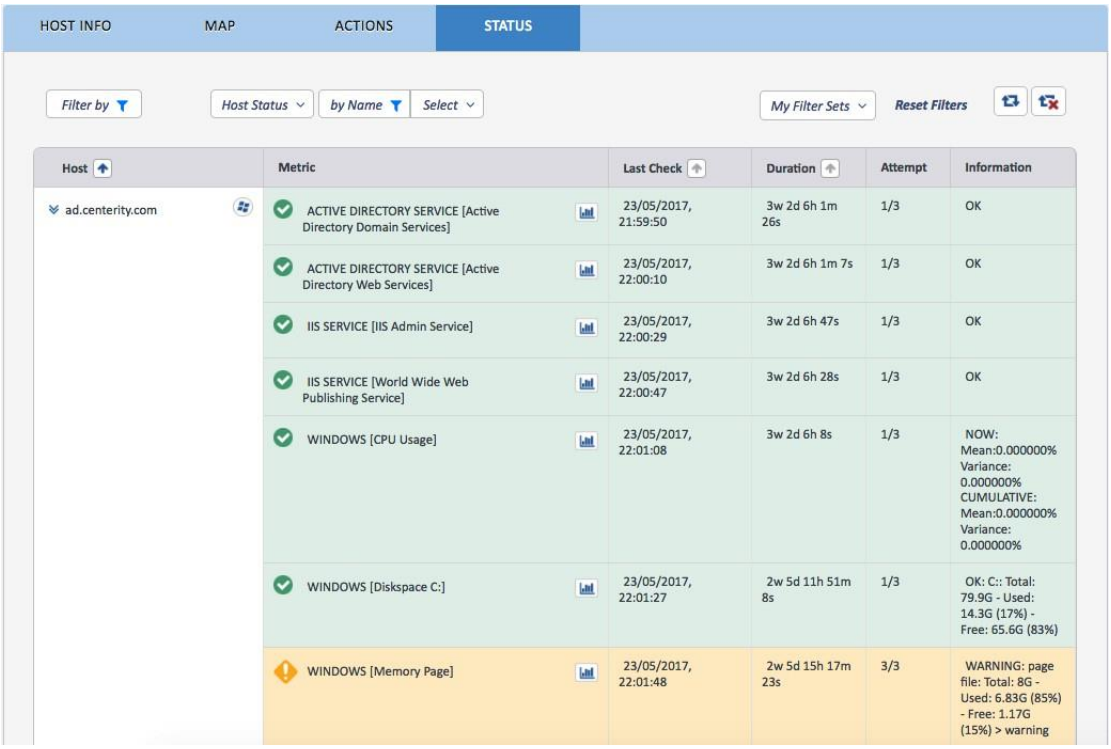
   iii. Disable notifications for all metrics: Stop metric notifications on the selected host-group

   iv. Enable checks of all metrics: Enable checks for all metrics on the selected host-group.

   v. Disable checks of all metrics: Disable checks from executing for the selected host-group.

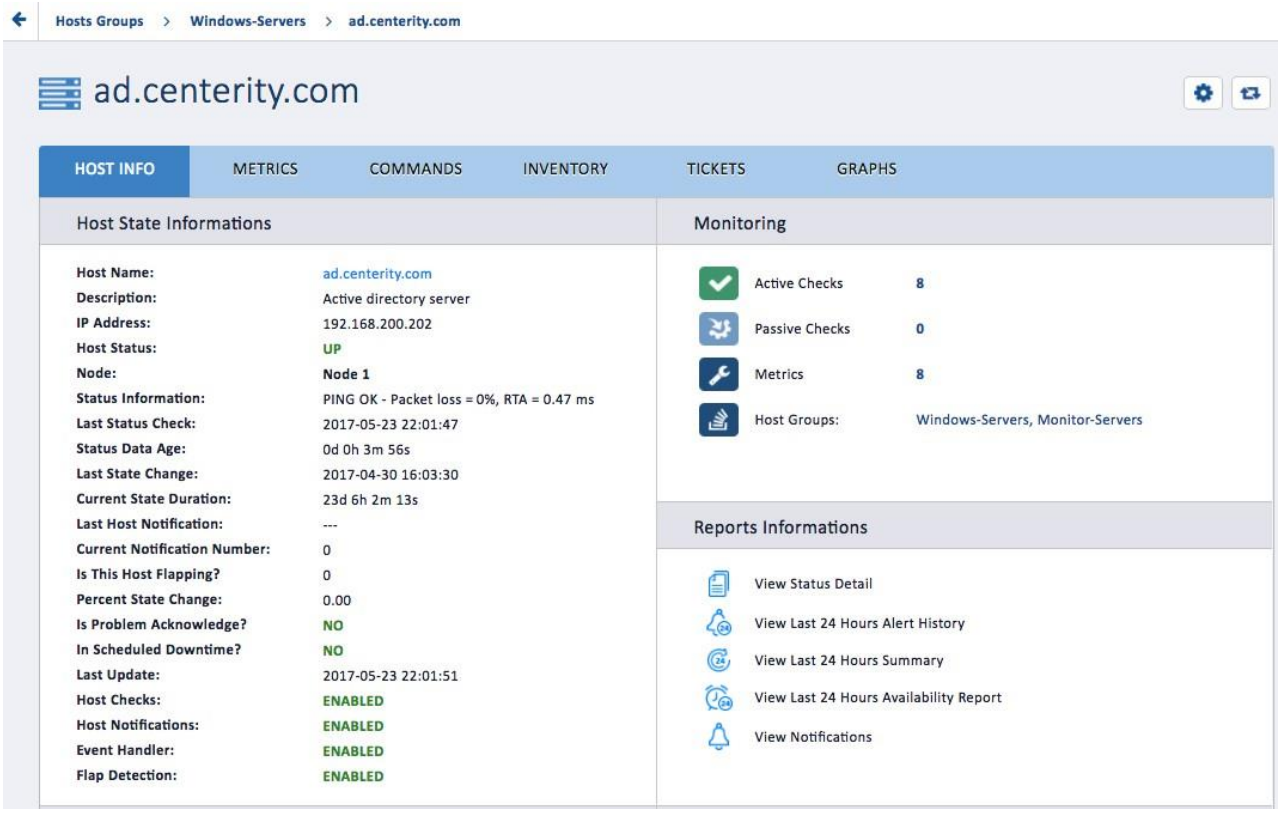
4. **Status**:

   Displays all hosts checks under that host group

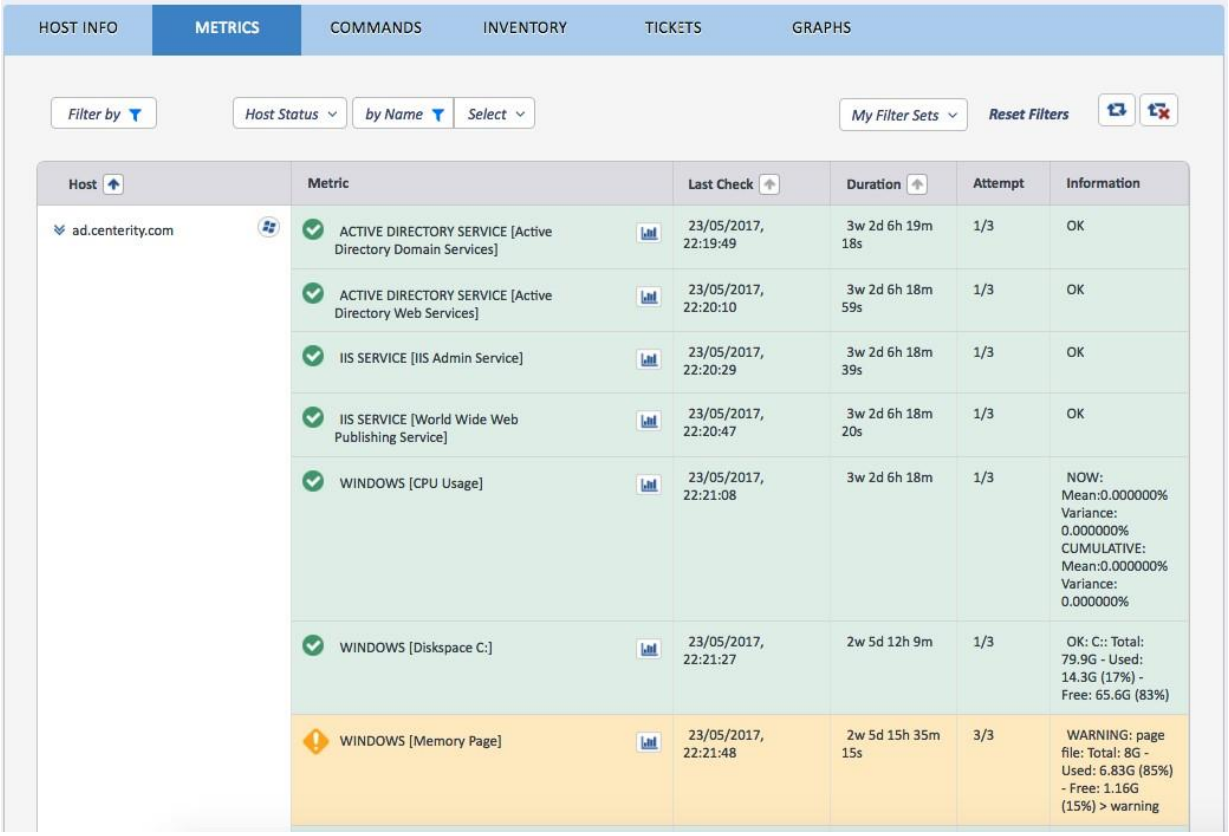


5.3 Host Management

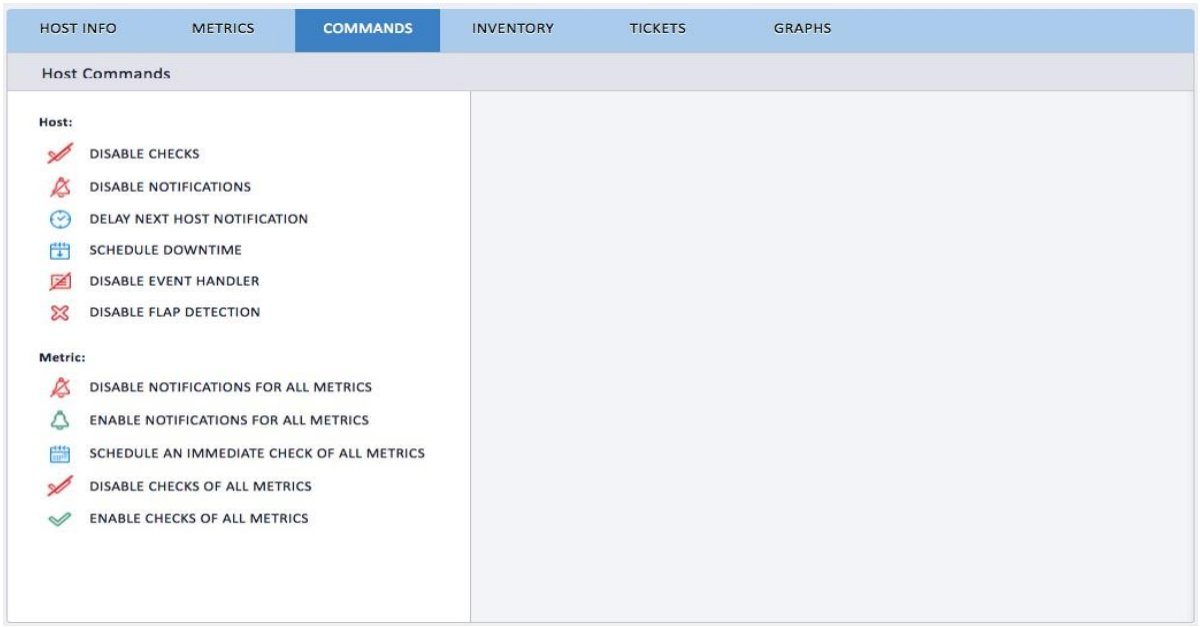
By clicking on a host name, the page redirects to host management page:



1. **Host Info**: Displays host state information, metric statistics, availability data and a reporting option:
   a. **View Status Detail**: Redirects to host events.
   b. **View Last 24 Hours Alert History**: Generate history report on the host for the last 24-hours.
   c. **View Last 24 Hours Summary**: Generates a Summary report for the host for the last 24-hours.
   d. **View Last 24 Hours Availability Report**: Generates availability report on the host for the last 24-hours.
   e. **View Notifications**: Displays all metric notifications generated from the host.
2. **Metrics**: Displays all host checks:



3. **Commands**:



a. **Host**:

i. **Disable checks**: Disable the host checks.

ii. **Disable notifications**: Disable host notifications.

iii. **Delay next host notification**: Delay next host notification in minutes.

iv. **Schedule Downtime**: Schedule host downtime.

v. **Disable event handler for this host**: Prevents Centerity Monitor from running the host event handlers on the selected host.

vi. **Disable flap detection for this host**: Disable flap detection for the selected host.

b. **Metric**:

i. **Disable notifications for all metrics**: Disable metric notifications.

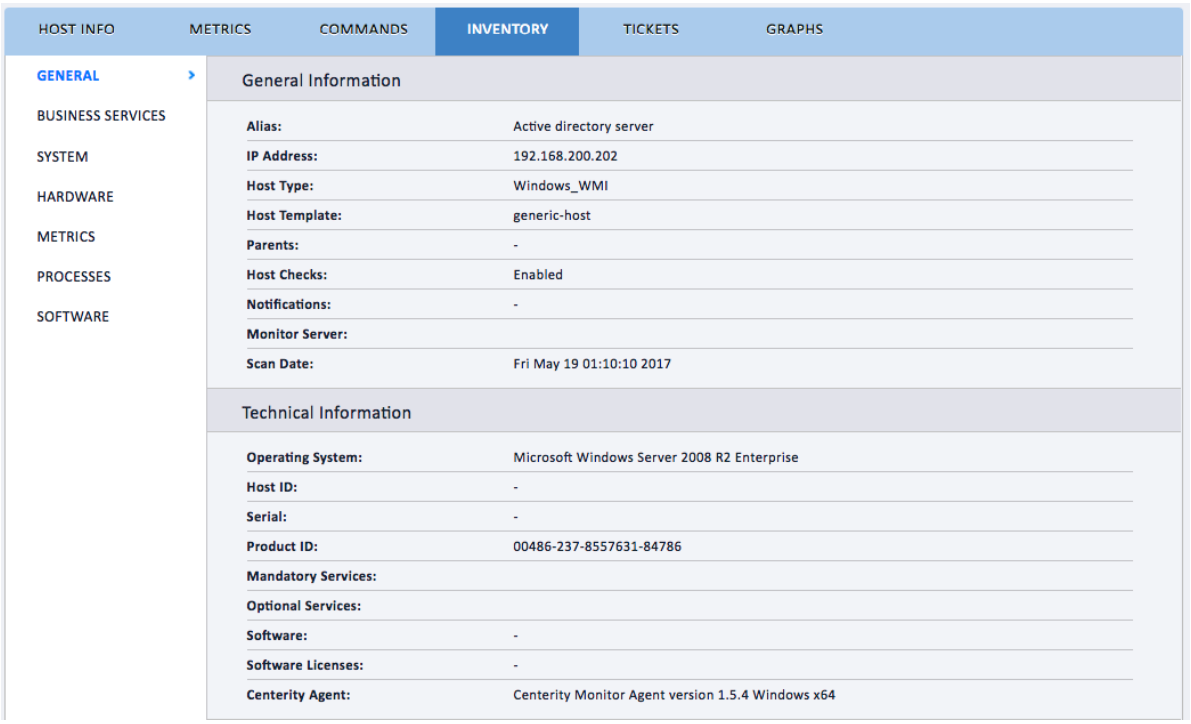
ii. **Enable notifications for all metrics**: Enable notifications.

iii. **Schedule an immediate check for all metrics**: Schedule the next check of all metrics on the selected host. When selecting “force check” option, the Monitor will force a check of all metrics on the host regardless of what time the scheduled checks occur and whether checks are enabled for those metrics.

iv. **Disable checks of all metrics**: Disable active checks of all metrics.

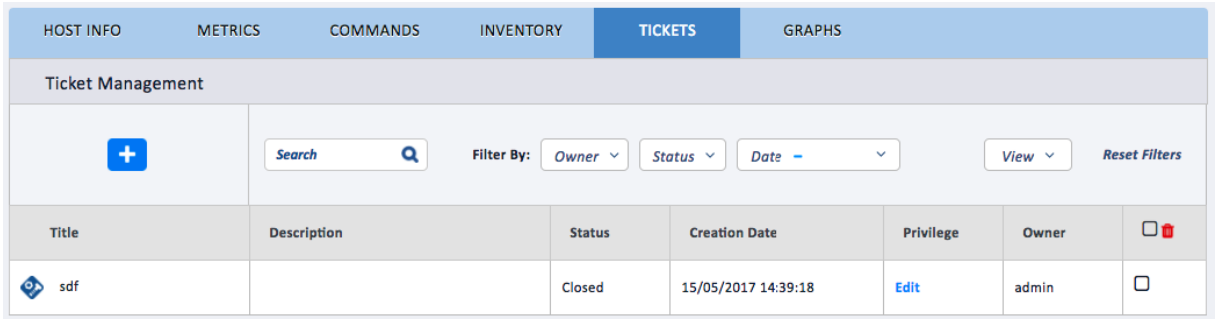
v. **Enable checks of all metrics**: Enable active checks of all metrics.

4. **Inventory**: Displays inventory information regarding the host such as: IP-address, OS, processes, services etc.



Note: Inventory requires a scan for Agent/WMI/VMware Inventory or any custom inventory.

5. **Tickets**: Centerity Monitor includes a minimal built-in ticketing system. It allows documenting and submitting information regarding specific hosts.



When clicking on the "+" sign, a new ticket opens.

a. **Title**: The title for the ticket.

b. **Description**: The description for the ticket.

c. **Type**: Incident / Note.

d. **Status**: Open / Closed / Ongoing.

e. **Priority:** Low / Medium / High / Urgent.

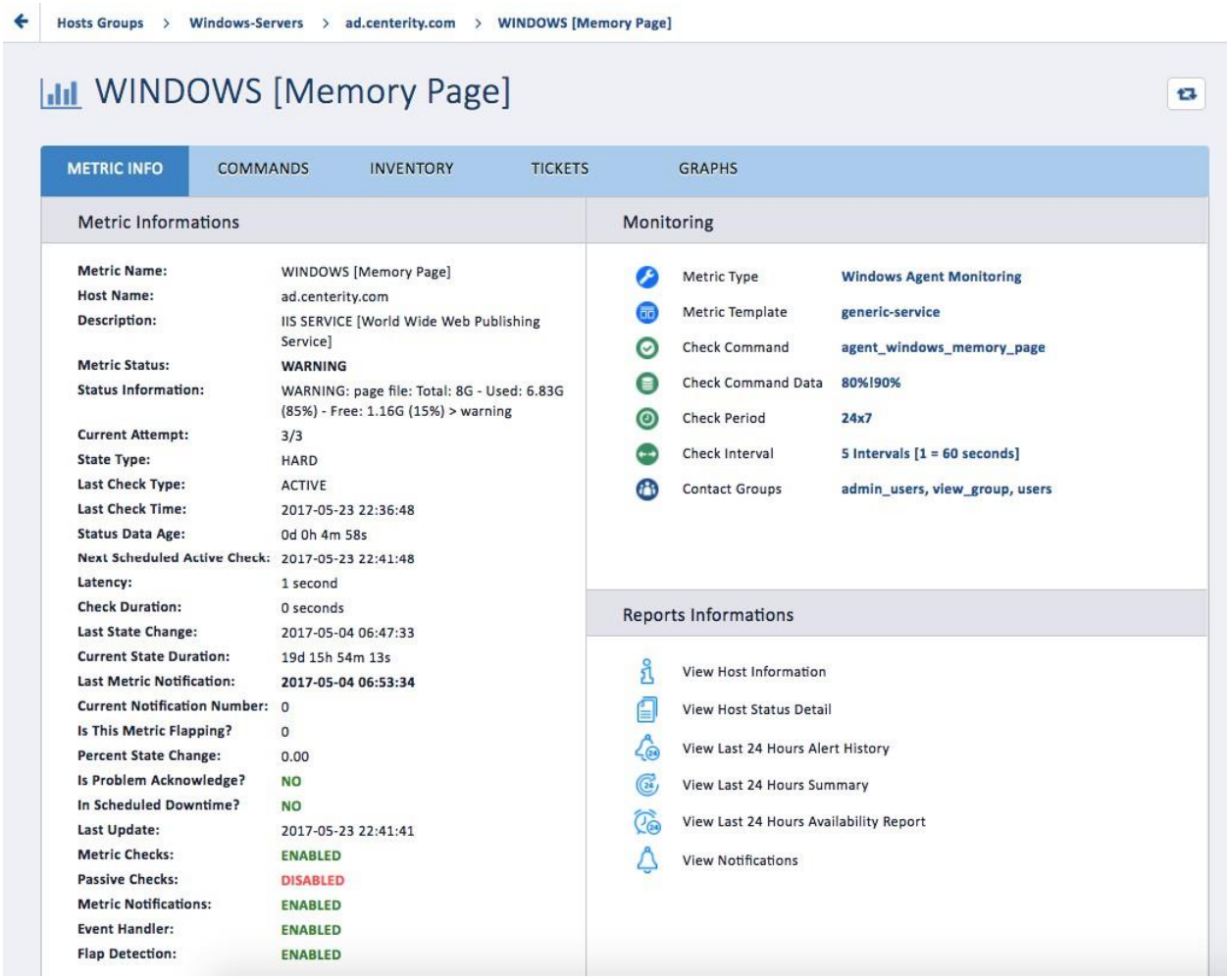
f. **Assigned to**: Users who can view/edit the ticket.

g. **Assigned to Contact Group**: Contact groups that can view/edit the ticket.

6. **Graphs**: This page displays all graphs associated with the host – double click will navigate to metric graphs page with extended graph history.

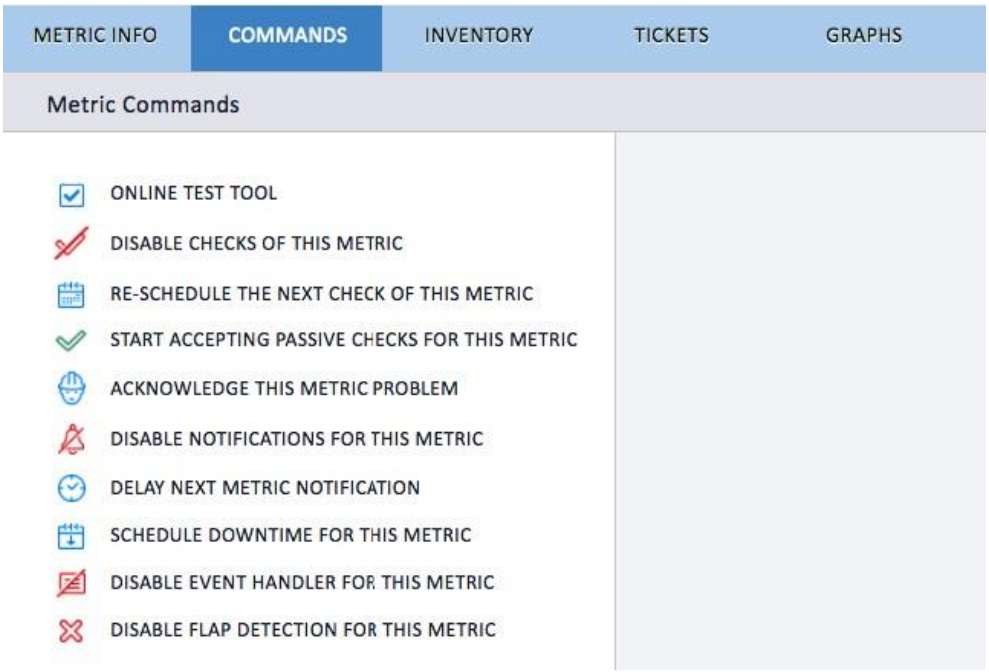
6. Metrics

By clicking on a metric name, the page redirects to metric management page:



1. **Status**: Displays metric state information, metric statistics, availability data and a reporting options:
   a. **View Host Information**: Redirects to host management.
   b. **View Host Status Detail:** Redirects to host events.
   c. **View Last 24 Hours Alert History**: Generate history report on the metric for the last 24-hours.
   d. **View Last 24 Hours Summary**: Generates a Summary report for the metric for the last 24-hours.
   e. **View Last 24 Hours Availability Report**: Generates availability report on the host for the last 24-hours.
   f. **View Notifications**: Displays all metric notifications generated from the host.

2. **Commands**:



a. **Online Test Tool**: Tests the check command.

b. **Disable checks for this metric**: Disable the metric checks on the metric.

c. **Re-schedule next check of this metric**: Schedules an immediate check for this metric.

d. **Start accepting passive checks for this metric**: Appears when passive checks are disabled. Enables passive checks.

e. Submit passive check result for this metric: Appears when passive checks are enabled. Submit a faux check result.

f. Stop accepting passive checks for this metric: Appears when passive checks are enabled. Disables passive checks.

g. **Acknowledge this metric problem**: Displayed only when the metric is in a non-OK state. Allows acknowledging the problem and type in a comment. The comment is sent out as a notification and will be displayed in System è Acknowledgement.

h. **Disable notifications for this metric**: Disable notifications on the metric.

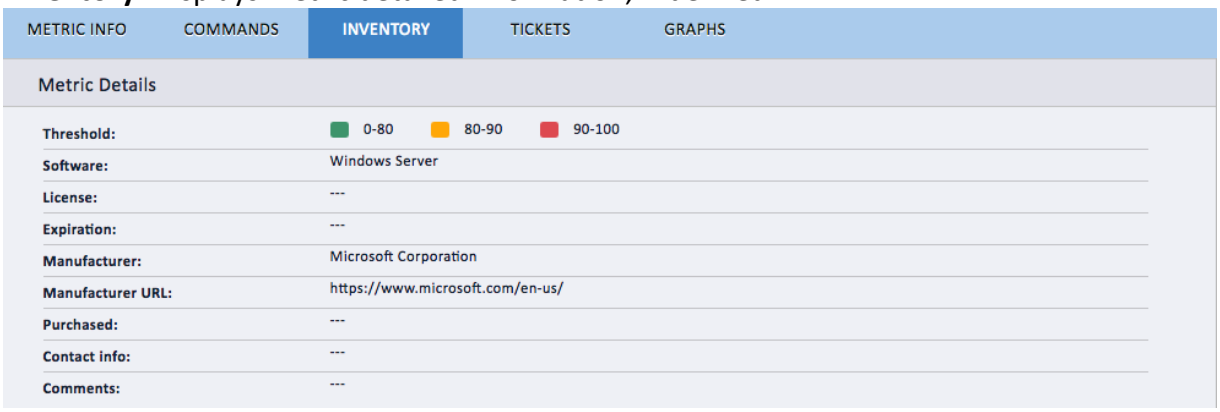
i. **Delay next metric notification**: Delay next host notification (minutes).

j. **Schedule downtime for this metric**: Schedule downtime on the selected host.

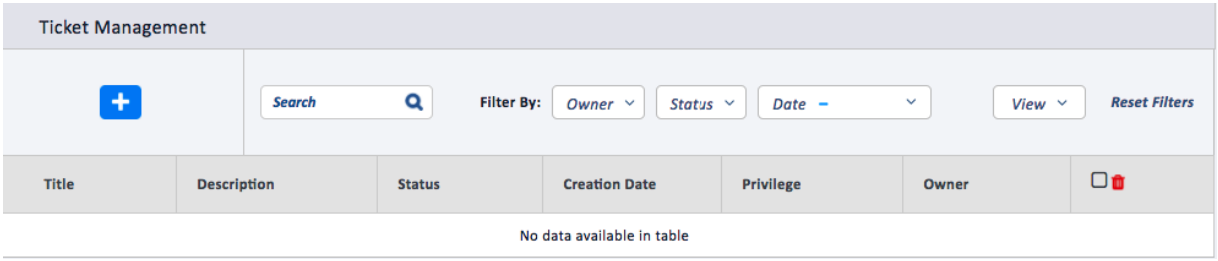
k. **Disable event handler for this metric**: Prevents running the metric event handlers on the selected metric.

l. **Disable flap detection for this metric**: Disable flap detection for the selected metric.

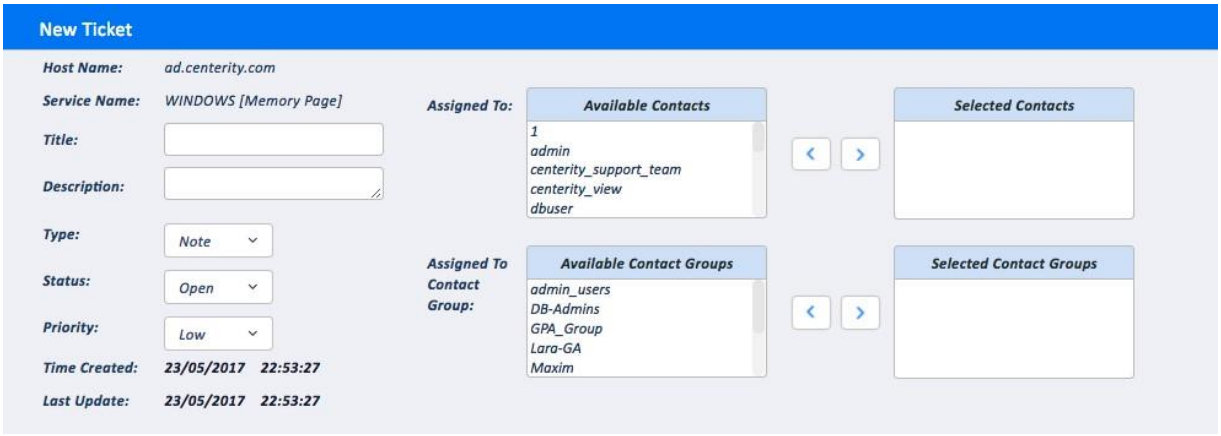
3. **Inventory**: Displays metric detailed information, if defined.



Tickets: Centerity Monitor includes a minimal built-in ticketing system. It allows to document and submit information regarding specific metrics.



When clicking on the "+" sign, a new ticket opens.



a. **Title**: The title for the ticket.

b. **Description**: The description for the ticket.

c. **Type**: Incident / Note.

d. **Status**: Open / Closed / Ongoing.

e. **Priority**: Low / Medium / High / Urgent.

f. **Assigned to**: Users who can view/edit the ticket.

g. **Assigned to Contact Group**: Contact groups that can view/edit the ticket.

7. Business Services

7.1 Overview

Business Service Views are an effective approach for managing Information Technology (IT) from the perspective of the business. They can increase business value through better management of IT and processes. **Centerity Monitor** can build a logical map containing layers of components such as network, web services, databases, storage, etc.; then, **Centerity Monitor** calculates the Metric utilization overall and for every component layer.

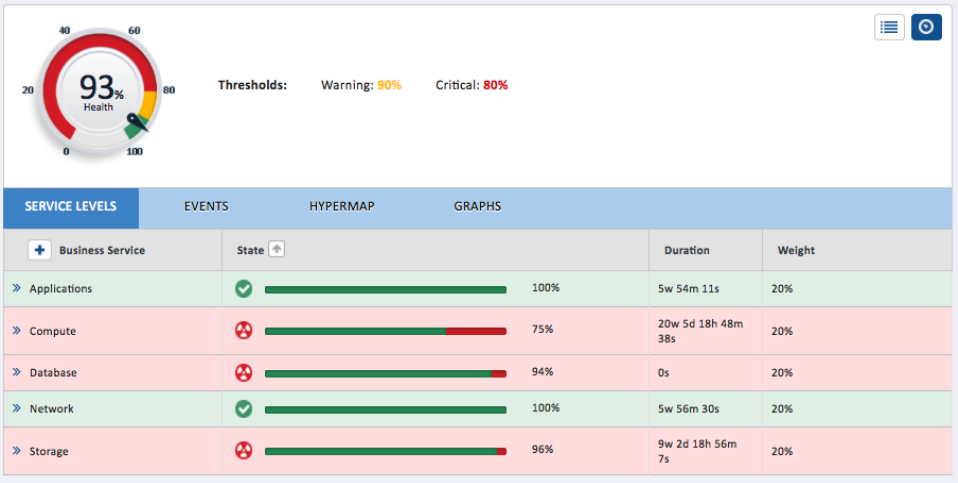
Business Service Management (BSM) leaves no stone unturned. Business services, activities, processes, transactions, etc. are understood from the business user's perspective, internally and externally. In their terms, their language and their performance expectations, while understanding the impact on their jobs, productivity, goals and objectives, SLAs, etc.

Monitor ➔ Dashboard ➔ Business Services: Displays all active Business Services in the system:

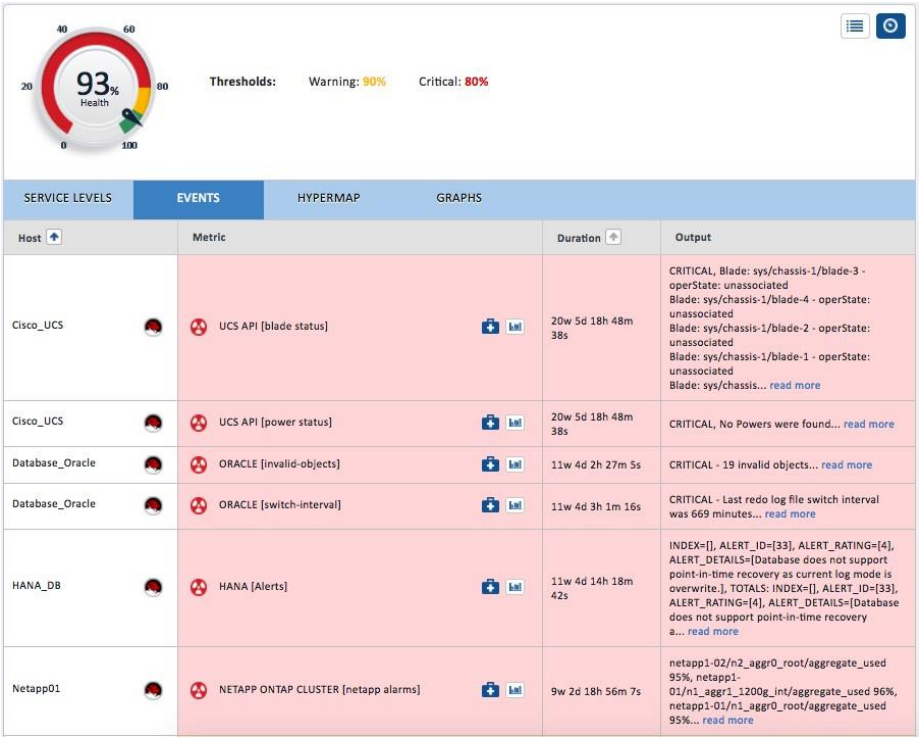
7.2 Detailed BSM information

Clicking on any of the Business Services will display more detailed information and drill down to the business service issues:

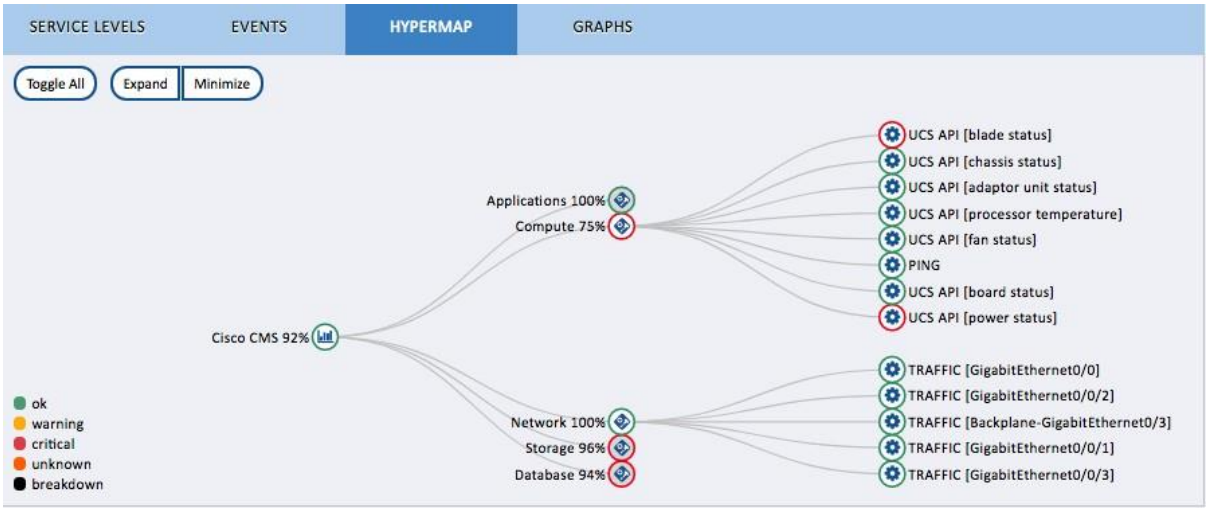
1. **Service Levels**: This view will display all levels in the business services, allowing to drill down to the problem using the button next to the name of the business service. The status column indicates issues with each level.



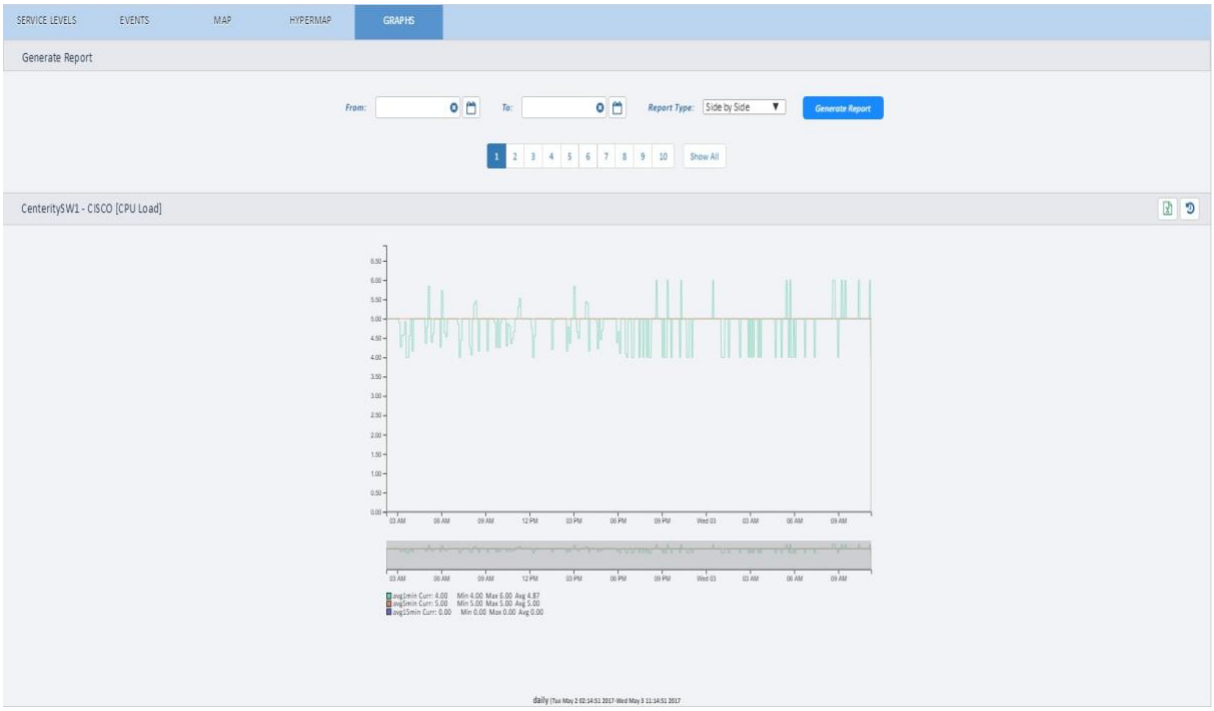
2. **Events**: Displays all current metric events on the business service.



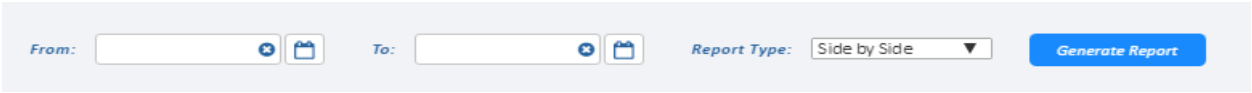
3. **Hyper Map**: Displays an automatic BSM hyper-map with all levels and metrics:



4. **Graphs**: All available BSM metric graphs:



a. **From/To**: Select the time-period of the graphs:



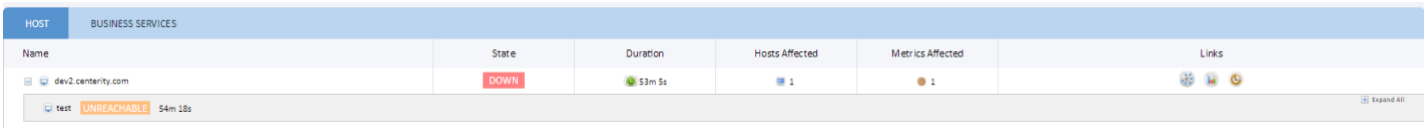
b. **Report Type**:

i. **Side by side**: Displays all graphs separated.

ii. **Combined Graph**: Displays a combined graph with a deselect option for unwanted metrics.

8. Root Cause Analysis

Centerity Monitor can detect breakdowns and outages of hosts. To do so, admins need to implement a Parent/Child relationship for every host that is monitored in the system or run a topology scan. Based on the relationships, Centerity Monitor will know which host affects which and can calculate the breakdowns more accurately.



The Network Outages view is accessed from Monitor è Outages.

1. **Name**: Name of the host causing the network outage.
2. **State**: State of the host.
3. **Duration**: How long has the outage been happening.
4. **Hosts Affected**: Number of hosts affected by the outage.
5. **Metrics Affected / Business Service Affected**: Number of metrics / business service affected by the outage.
6. **Links**: Perform various actions and view reports on the specific outage:
   a. **Map** : Displays outages map.
   b. **Availability** : Displays last 24-hours availability report for this host.
   c. **History** : Displays last 24-hours history report for tis host.

9. Status Map

9.1 Overview

A network diagram is important to visualize problems in the network. Centerity Monitor provides 3 types of map:

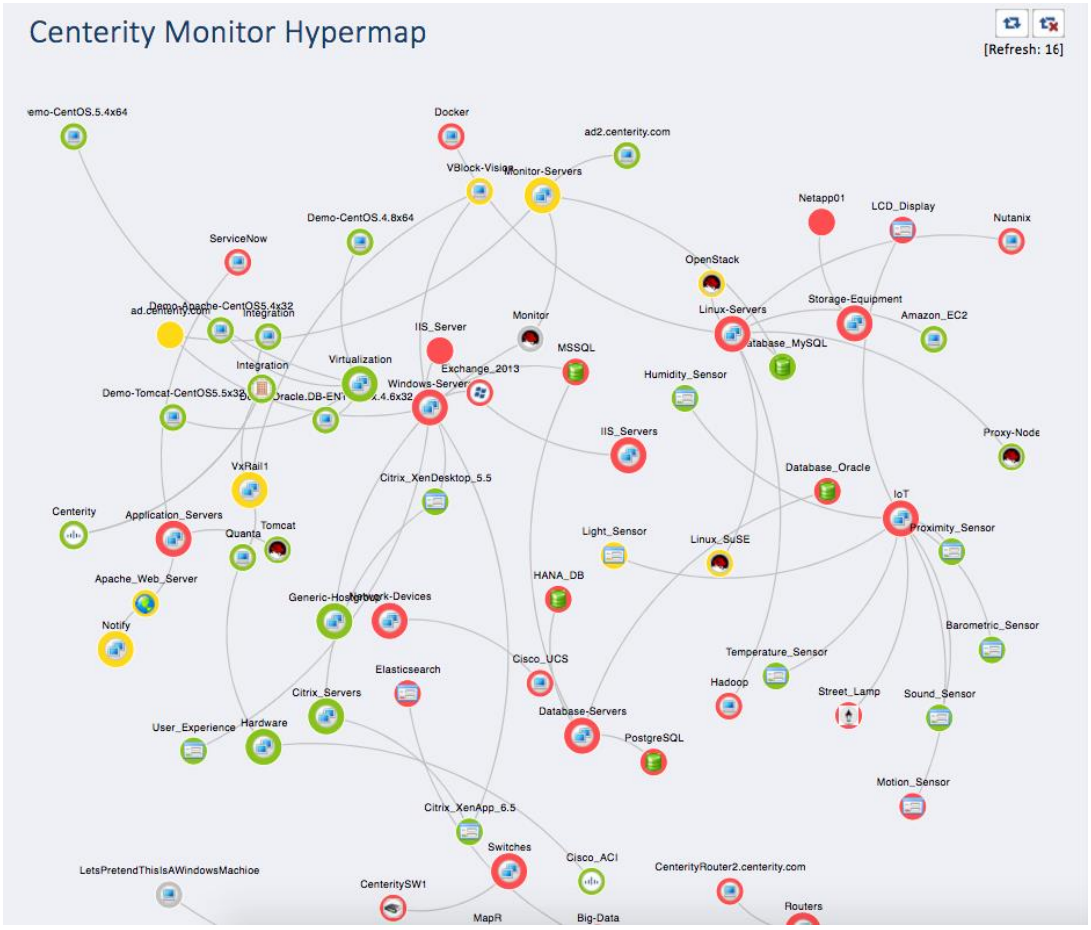
1. Hyper Map
2. Topology map
3. Live Network map

The Hyper Map and Topology map will be created automatically based on hierarchy definition ant parent-child relationship in the topology scan.

9.2 Visual Layouts - Hypermap

Under Monitor ➔ Maps ➔ Hyper Map on the top right.

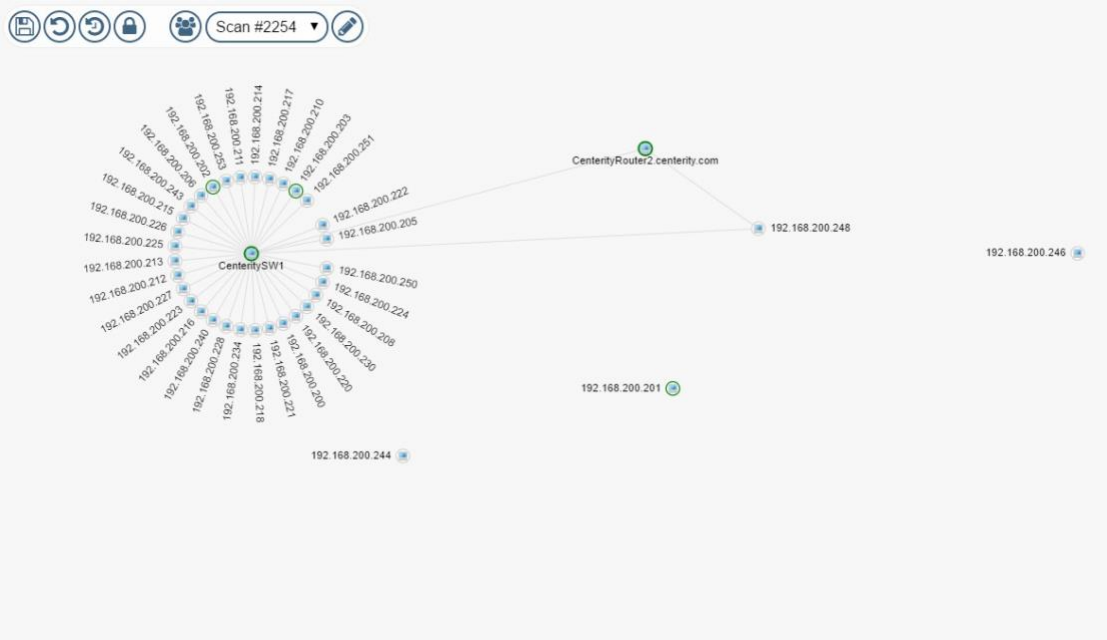
The Hyper map provides dynamic and interactive network layout. By default, all hosts that are defined in the system will be presented in the hyper map.



9.3 Topology Map

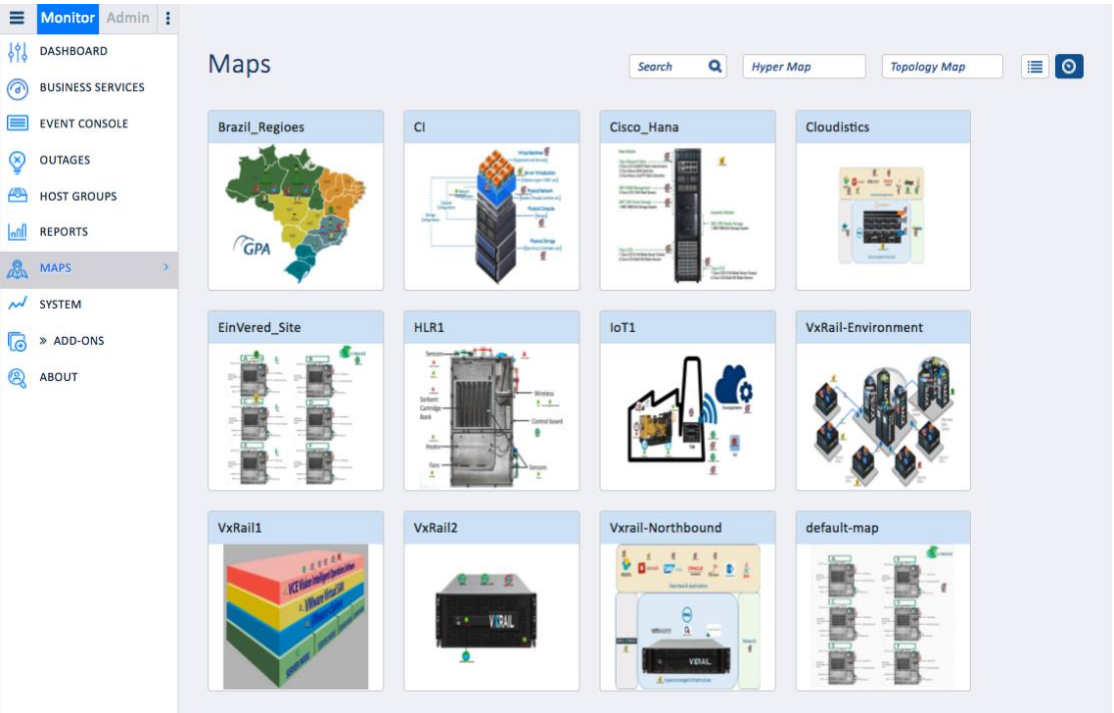
Under Monitor ➔ Maps ➔ Topology Map on the top right.

The topology map provides real-time indication about problems with the metrics in every host on the map. In the topology-map page, the map name can be changed, the map can be merged with another map, show the last 10 scans and set the primary map.



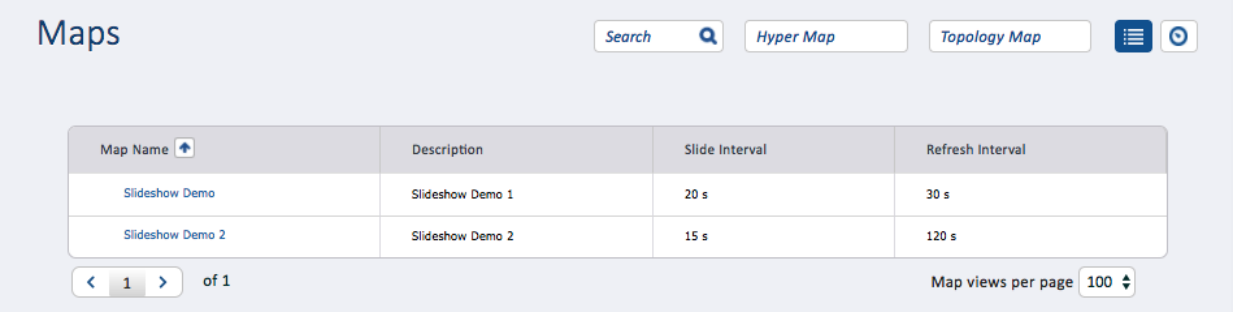
9.4 Maps Dashboard

Displays all custom maps created by admins:



9.5 Visual Layouts – Maps Views

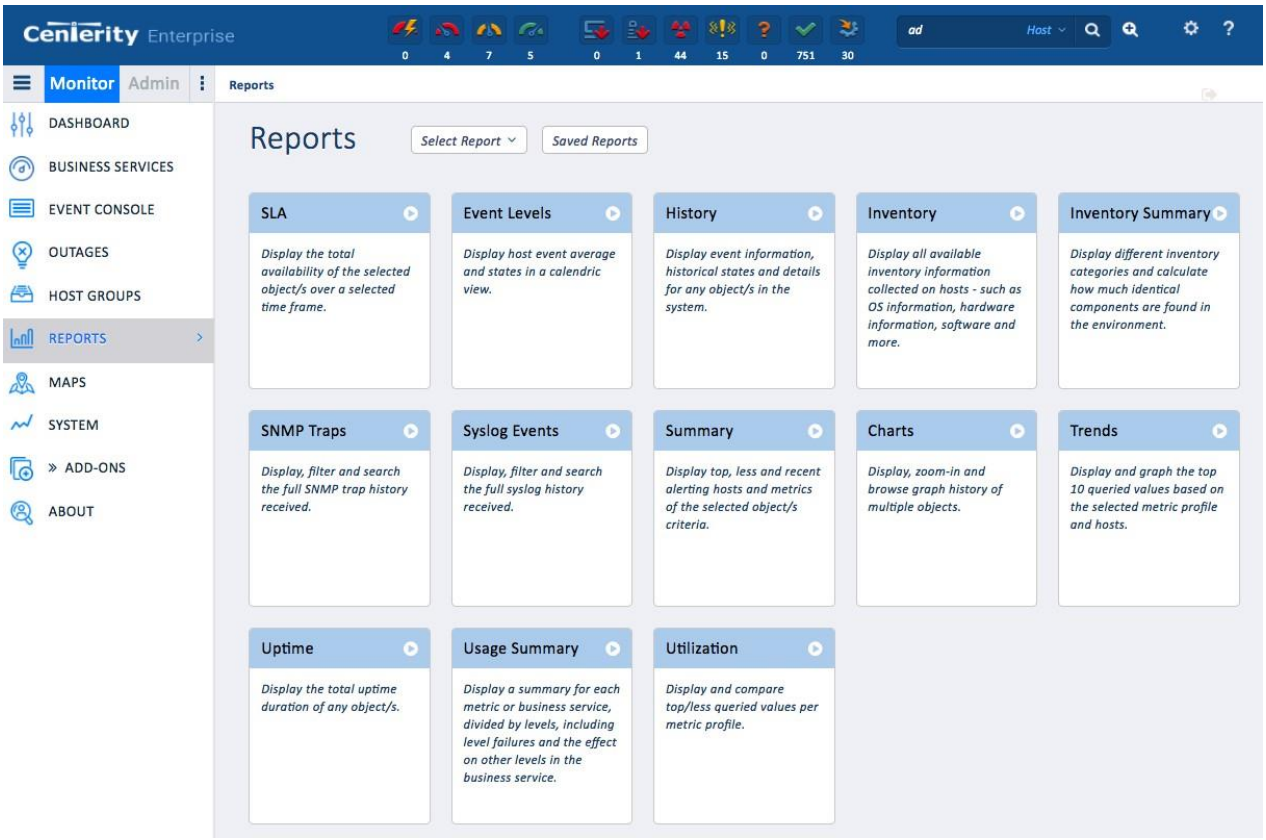
Displays all maps views created by admins:



10. Reports

10.1 Reports Options

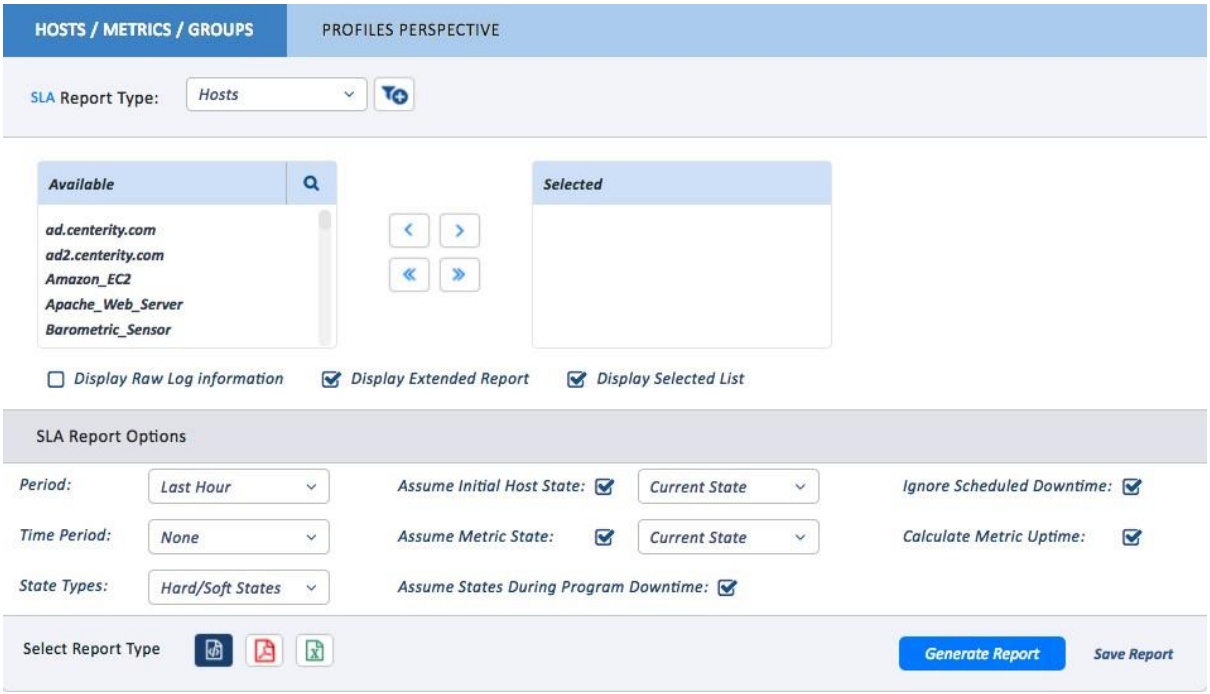
Centerity Monitor provides wide range of professional built-in reports. Each report can be saved as excel, pdf or generated in HTML format.



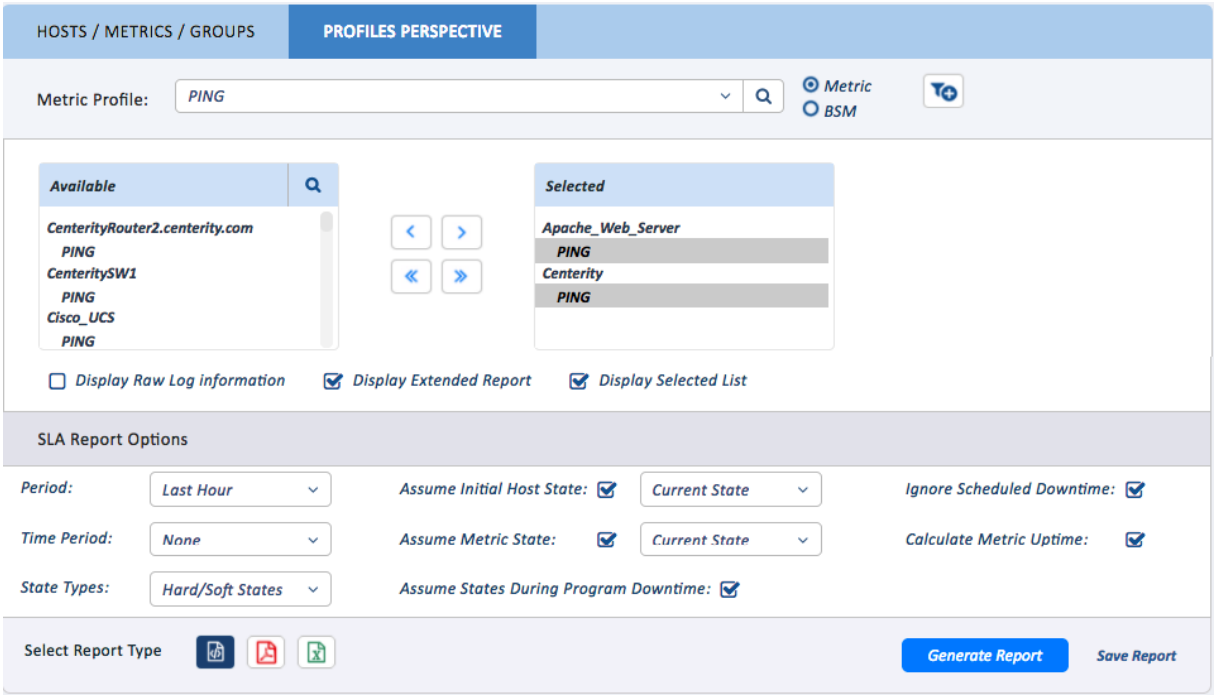
10.1.1 SLA Report

Display the total availability of the selected object/s over a selected time frame.

The report wizard includes the following options:



1. **Perspective type**: there are 4 options for this report. In each one - select the object from the left box and use the arrow to move into the right box.
   a. **Host / Metric / Group**:
      i. **Host/Hosts** availability
      ii. **Metric / Metrics availability**
      iii. **Host group** availability
      iv. **Business Service** availability (BSM)
   b. **Profile Perspective**: Allows availability by selected metric profile:
      i. **Metric**: Displays the metric profile within hosts.
      ii. **BSM**: Displays the metric profile within business services.



- **Display Raw Log information**: Displays event history log.
- **Display Extended Report**: Displays time duration of downtime as well as availability percentage.
- **Display Selected List**: Display/Don't display the host list in a PDF export.
- **Report Period**: Choose from a set of predefined report periods or choose "CUSTOM REPORT PERIOD" and specify Start and End date.

c. Start Date (Inclusive): Specify Start Date if "CUSTOM REPORT PERIOD" was selected above.

d. End Date (Inclusive): Specify End Date if "CUSTOM REPORT PERIOD" was selected above.

2. **Report Time-Period**: What Schedule Time-period the report is created for.

   i. **Ignore Scheduled Downtime**: The report will ignore any scheduled downtime on the host/metric.

   ii. **Calculate Metric Uptime**: The report will display current uptime for this host.

   iii. **Assumed Initial Host State**: If there is no information about the host or metric in the current log file, Centerity Monitor can assume status of the host/metric. Default value is "Current State".

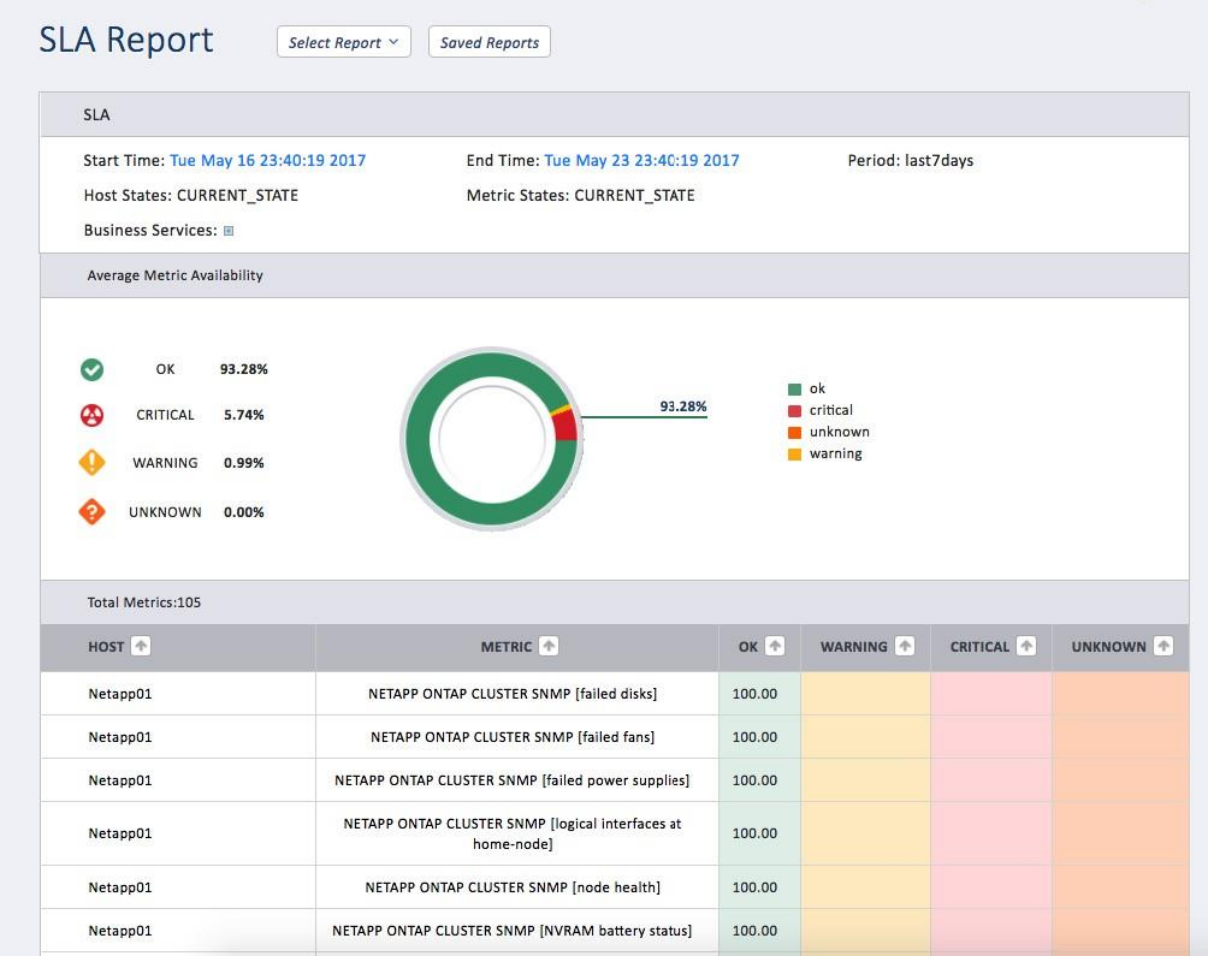
3. **Assume Metric State**: If there is no information about the host or metric in the current log file, Centerity Monitor can assume status of the host/metric. Default value is "Current State".

4. **State Type**: A problem is classified as a SOFT problem until the number of checks has reached the configured max check attempts value (Default: 3). When max check attempts are reached,

the problem is reclassified as HARD and Centerity Monitor will send out a notification about the problem. SOFT problems do not result in notifications.

5. **Assume States During Program Downtime**: If Centerity Monitor is not running for some time during a report period this will assume states for hosts and metrics during the downtime.

   Example of "Last 7 Days BSM" report:



10.1.2 Event Level Report

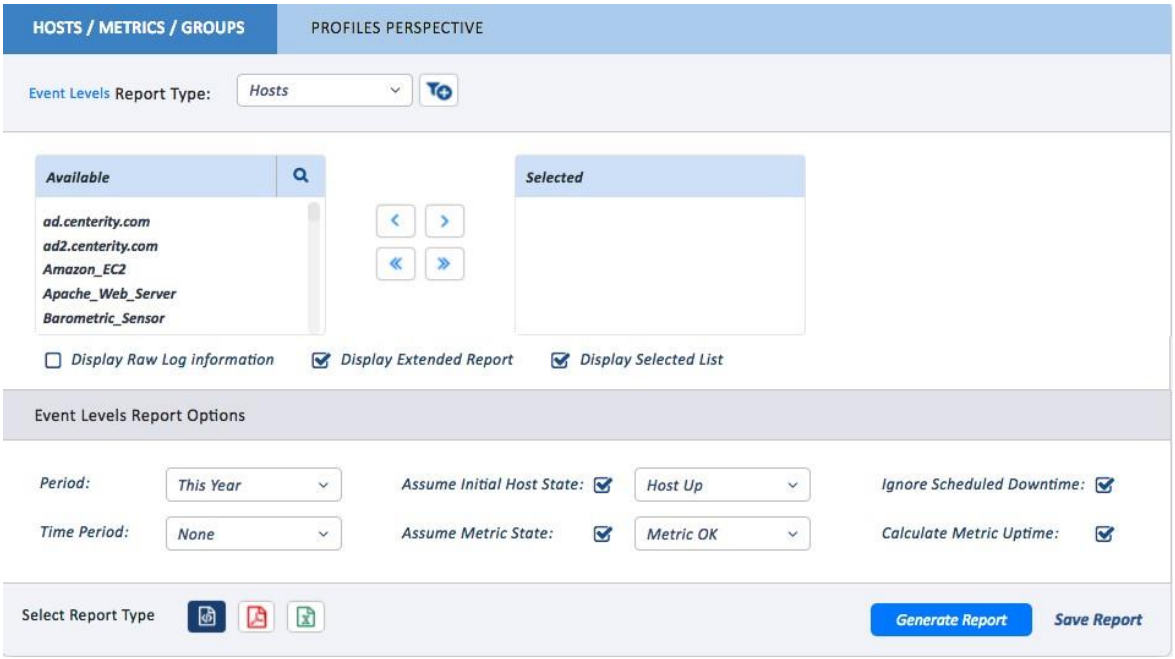
The event level report shows period averages and host events in calendric view.

1. **Perspective type** - there are 4 options for this report. In each one - select the object from the left box and use the arrow to move into the right box.
   a. **Host / Metric /Group**:
      i. **Host/Hosts** averages
      ii. **Metric/Metrics** averages
      iii. **Host group** averages
      iv. **Business Service** averages (BSM)

b. **Profile Perspective**: Allows averages by selected metric profile:

i. **Metric**: Displays the metric profile within hosts.

ii. **BSM**: Displays the metric profile within business services.



iii. **Display Raw Log information**: Displays event history log.

iv. **Display Extended Report**: Displays time duration of downtime as well as availability percentage.

v. **Display Selected List**: Display/Don't display the host list in a PDF export.

c. **Report Period**: Choose from a set of predefined report periods or choose "CUSTOM REPORT PERIOD" and specify Start and End date.

i. **Start Date** (Inclusive): Specify Start Date if "CUSTOM REPORT PERIOD" was selected above.

ii. **End Date** (Inclusive): Specify End Date if "CUSTOM REPORT PERIOD" was selected above.

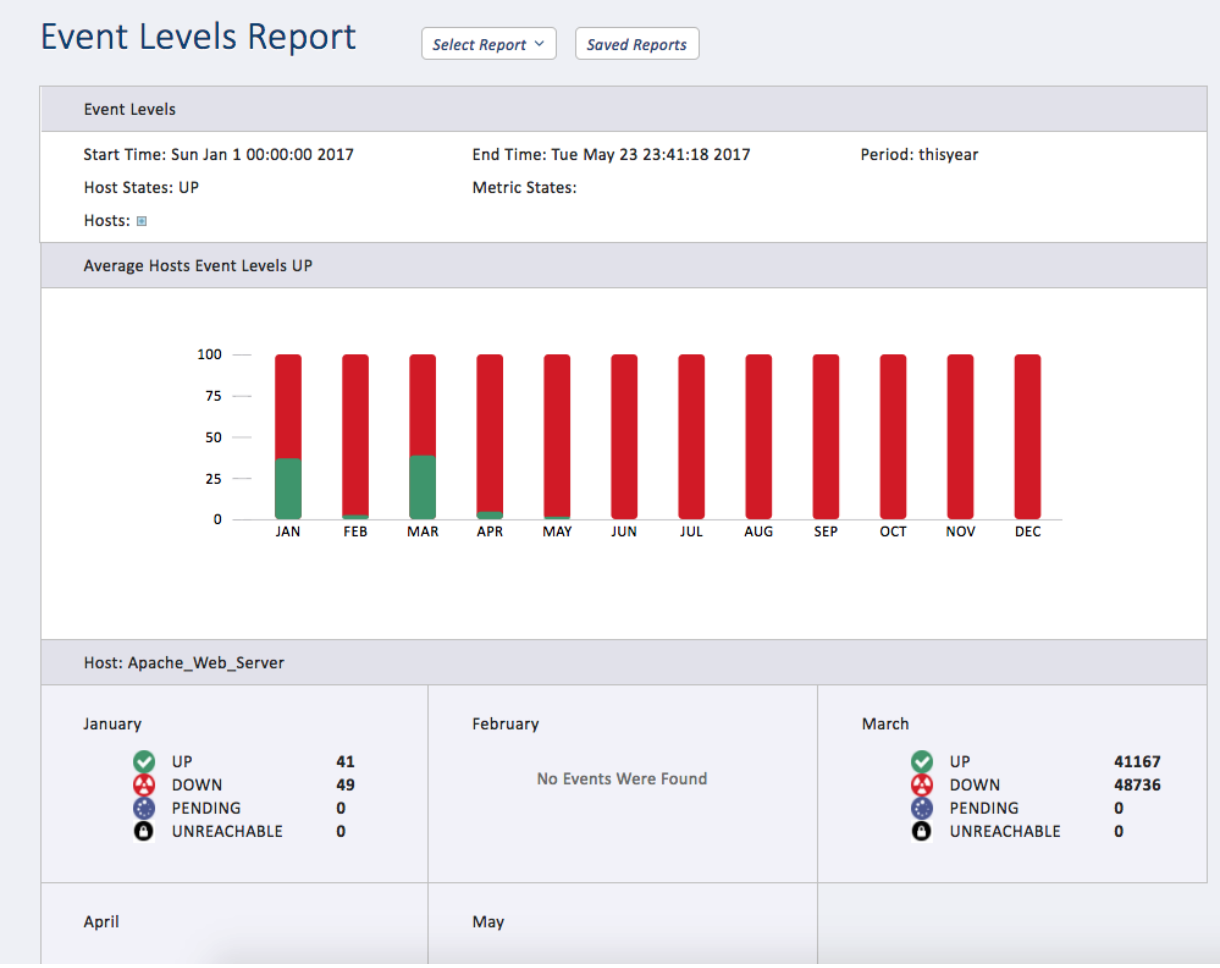
iii. **Report Time-Period**: What Schedule Time Period the report is created for.

iv. **Ignore Scheduled Downtime**: The report will ignore any scheduled downtime on the host/metric.

v. **Calculate Metric Uptime**: The report will display current uptime for this host.

vi. **Assumed Initial Host State**: If there is no information about the host or metric in the current log file, Centerity Monitor can assume status of the host/metric. Default value is "Current State".

vii. **Assume Metric State**: If there is no information about the host or metric in the current log file, Centerity Monitor can assume status of the host/ metric. Default value is “Current State”.



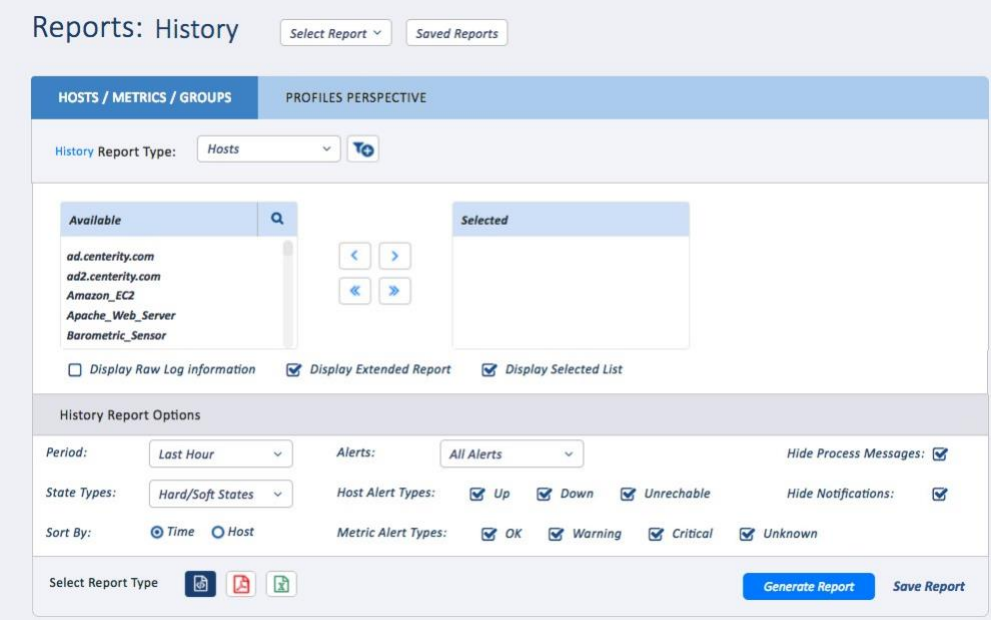
10.1.3 History Report

The history report presents detailed information about historical states of any element in the system with several of options. This report can be saved as PDF and to be sent automatically by email.

1. **Perspective type** - there are 4 options for this report. In each one - select the object from the left box and use the arrow to move into the right box.
   a. **Host / Metric /Group**:
      i. **Host/Hosts** event history
      ii. **Metric/Metrics** event history
      iii. **Host group** event history
      iv. **Business Service** event history (BSM)
   b. **Profile Perspective**: Allows history report by selected Metric profile:

i. **Metric**: Displays the metric profile within hosts.

ii. **BSM**: Displays the metric profile within business services.



iii. **Display Raw Log information**: Displays event history log.

iv. **Display Extended Report**: Displays time duration of downtime as well as availability percentage.

v. **Display Selected List**: Display/Don't display the host list in a PDF export.

c. **Report Period**: Choose from a set of predefined report periods or choose "CUSTOM REPORT PERIOD" and specify Start and End date.

i. **Start Date** (Inclusive): Specify Start Date if "CUSTOM REPORT PERIOD" was selected above.

ii. **End Date** (Inclusive): Specify End Date if "CUSTOM REPORT PERIOD" was selected above.

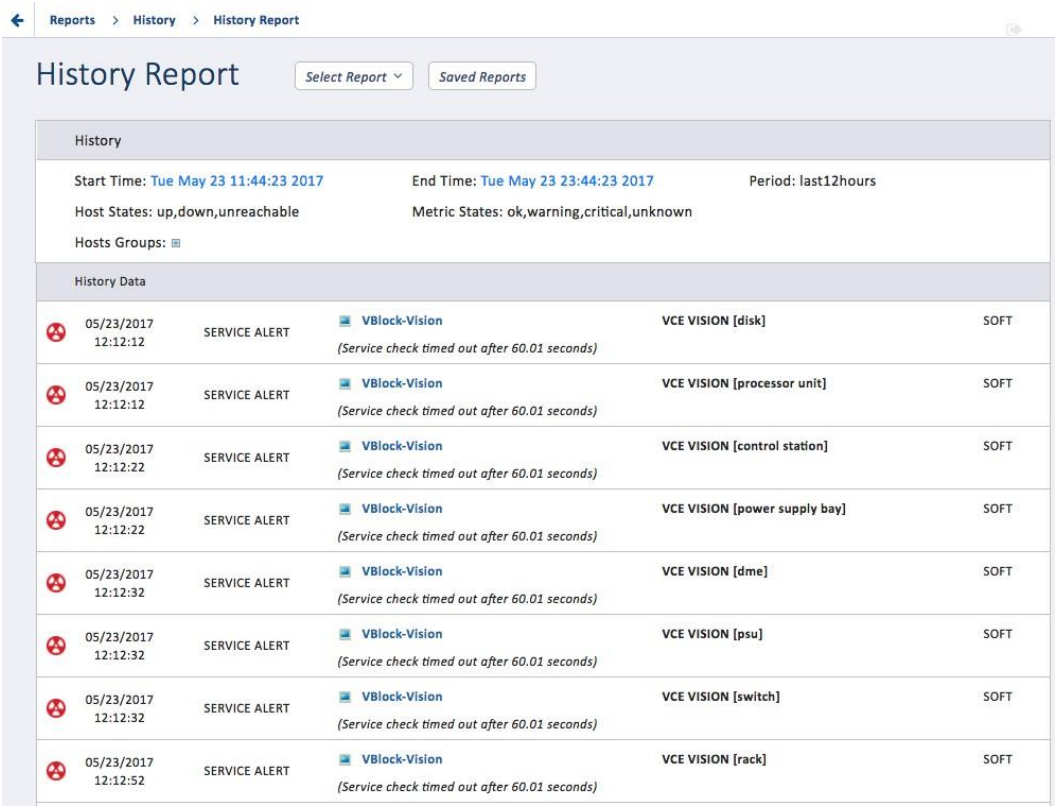
iii. **State Type**: A problem is classified as a SOFT problem until the number of checks has reached the configured max check attempts value (Default: 3). When max check attempts are reached, the problem is reclassified as HARD and Centerity Monitor will send out a notification about the problem. SOFT problems do not result in notifications.

iv. **Alerts**: Host alert/metric alerts.

v. **Host Alert Types**: The host alert types that will be displayed in the report.

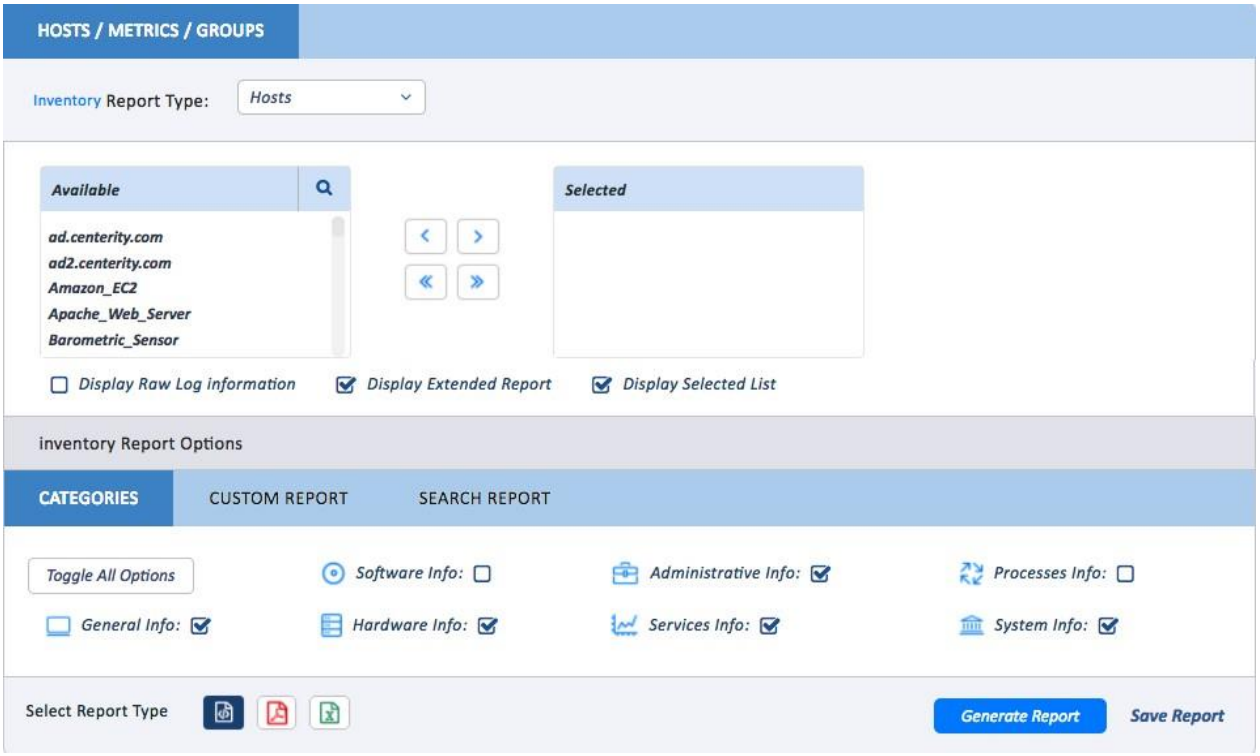
vi. **Metric Alert Types**: The metric alert types that will be displayed in the report.

vii. **Hide Process Messages**: Hides all process messages.



10.1.4 Inventory Report

Inventory report shows all available inventory information on hosts – such as OS information, hardware information, software details and more. This report depends on inventory scan, hosts that were not scanned properly will appear blank.



1. **Report type**: there are 2 options for this report. In each one - select the object from the left box and use the arrow to move into the right box.
   a. Host/Hosts inventory
   b. Host group inventory

   Display Raw Log information: Displays event history log.

   Display Extended Report: Displays time duration of downtime as well as availability percentage.

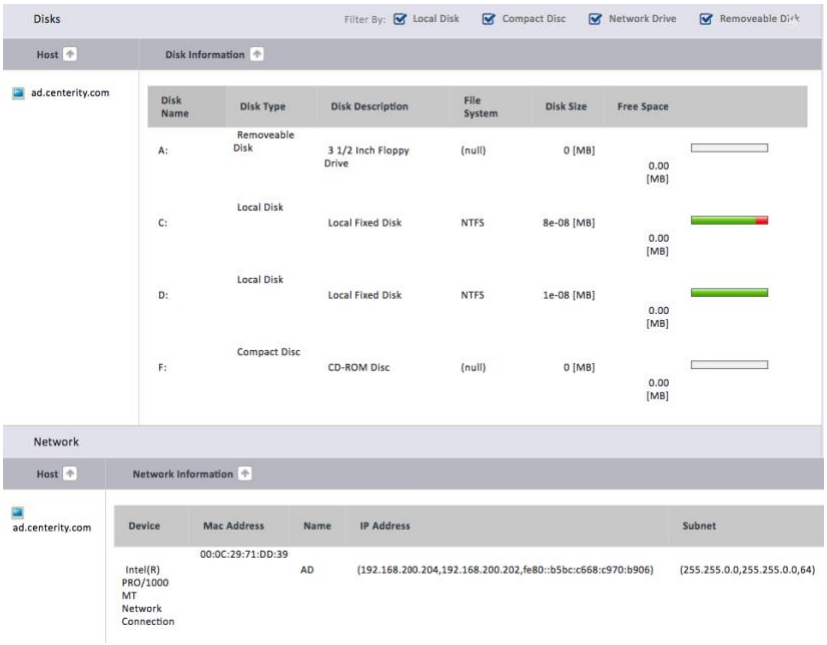
   Display Selected List: Display/Don't display the host list in a PDF export.

   Report Categories:

   a. **General Information**: IP address, host type, group and alias.
   b. **Administrative Information**: All general information, topology, OS information, monitoring information, hardware supplier information and any user defined information.
   c. **Metrics Information**: All metrics on the host and their state.
   d. **Software Information**: All programs installed on this host.
   e. **System Information**: System, domain, hardware, OS and location details.
   f. **Hardware Information**: Bios, processor, memory, disks and network details.
   g. **Process Information**: Running processes on the host.

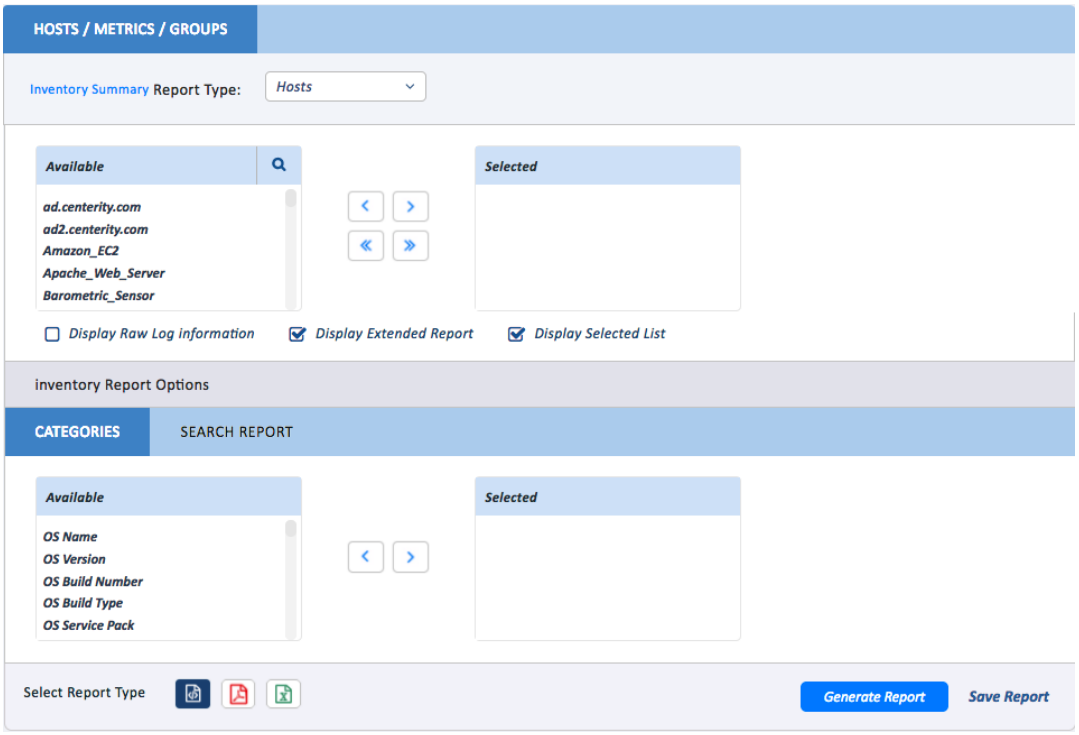
2. **Custom Report**:
   Allows you to select specific information you want from the host such as: OS Name, Domain, Host ID, etc.

3. **Search Report**:
   Allows you to define a search for a specific detail such as software, serial number, etc.



10.1.5 Inventory Summary Report

Summary inventory report can display how much of a certain software is installed on the environment, operating system etc. This report depends on inventory scan, hosts that weren't scanned properly will appear blank.



1. **Report type**: there are 2 options for this report. In each one - select the object from the left box and use the arrow to move into the right box.

   a. Host/Hosts inventory

   b. Host group inventory

   Display Raw Log information: Displays event history log.

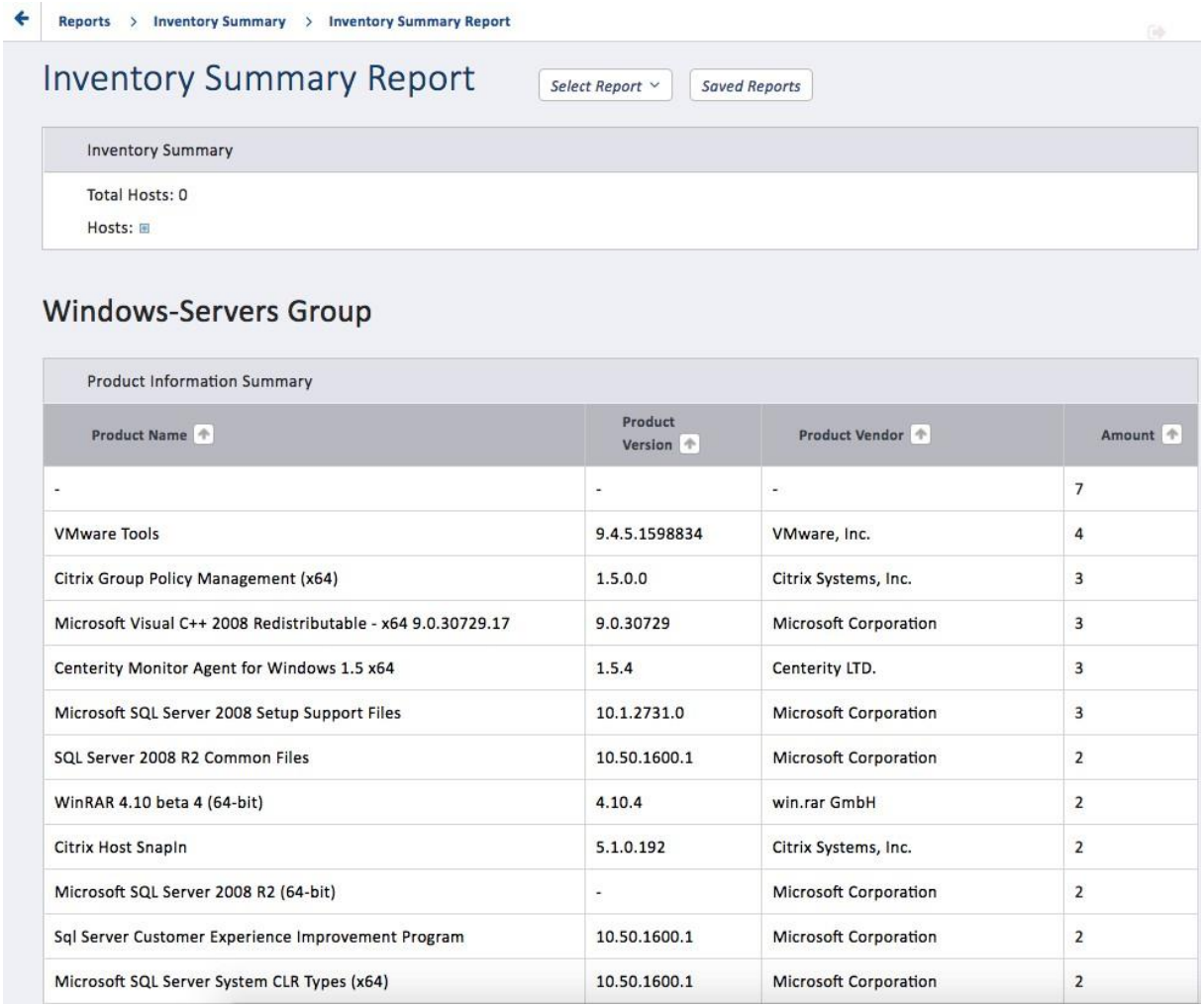
   Display Extended Report: Displays time duration of downtime as well as availability percentage.

   Display Selected List: Display/Don't display the host list in a PDF export.

   Select various settings for your report.

2. **Custom Report**:
   Allows you to select specific information you want from the host such as: OS Name, Domain, Host ID, etc.

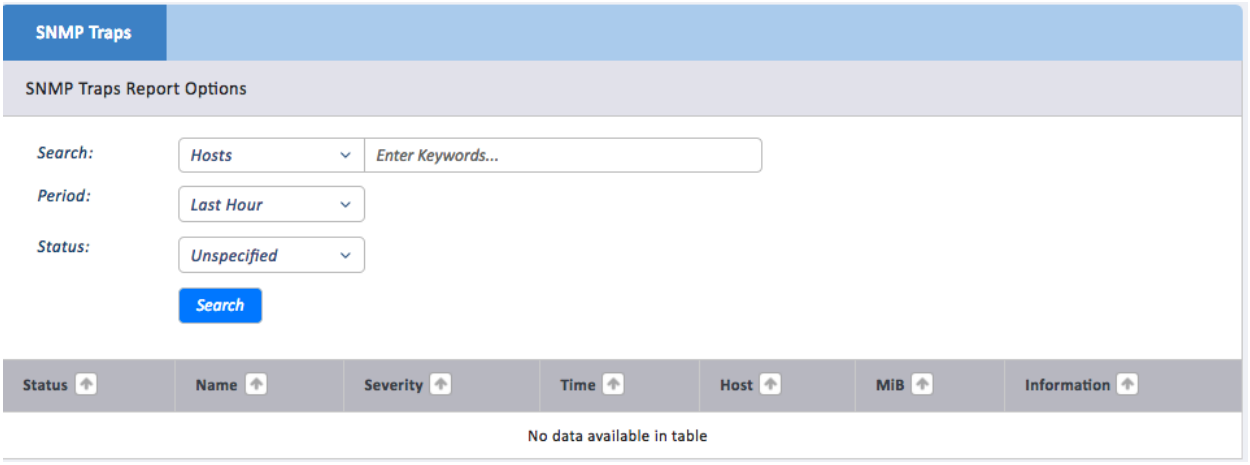
3. **Search Report**:
   Allows you to search for a specific detail within all hosts, such as software, serial number, etc.



Product Name	Product Version	Product Vendor	Amount
-	-	-	7
VMware Tools	9.4.5.1598834	VMware, Inc.	4
Citrix Group Policy Management (x64)	1.5.0.0	Citrix Systems, Inc.	3
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17	9.0.30729	Microsoft Corporation	3
Centerity Monitor Agent for Windows 1.5 x64	1.5.4	Centerity LTD.	3
Microsoft SQL Server 2008 Setup Support Files	10.1.2731.0	Microsoft Corporation	3
SQL Server 2008 R2 Common Files	10.50.1600.1	Microsoft Corporation	2
WinRAR 4.10 beta 4 (64-bit)	4.10.4	win.rar GmbH	2
Citrix Host SnapIn	5.1.0.192	Citrix Systems, Inc.	2
Microsoft SQL Server 2008 R2 (64-bit)	-	Microsoft Corporation	2
Sql Server Customer Experience Improvement Program	10.50.1600.1	Microsoft Corporation	2
Microsoft SQL Server System CLR Types (x64)	10.50.1600.1	Microsoft Corporation	2

10.1.6 SNMP Traps Report

SNMP Traps Report will display all SNMP trap history. It allows searching within the trap history and time period selection.

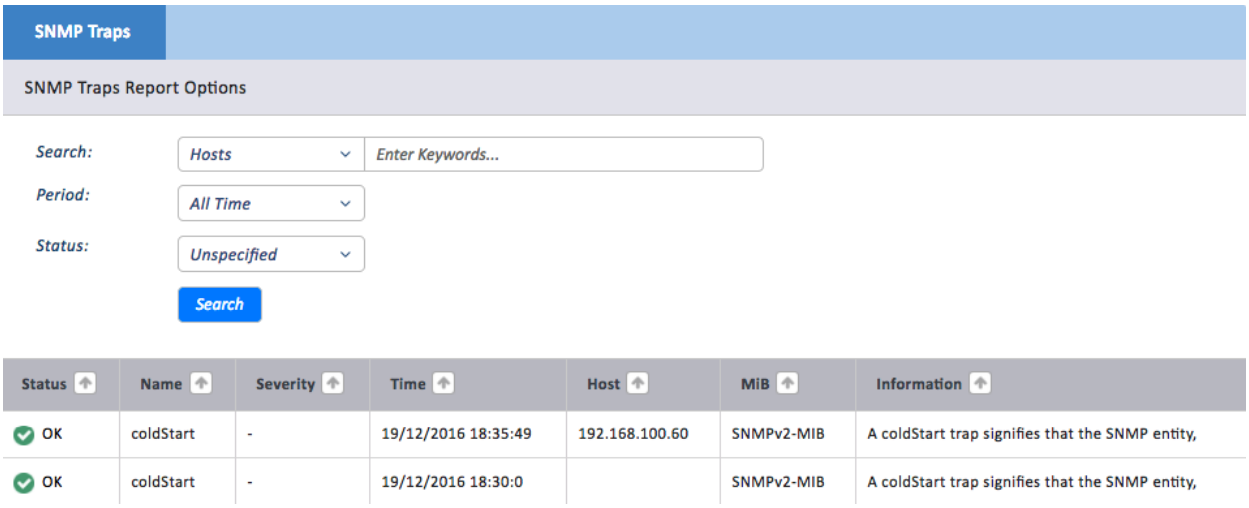


1. **Search**: Allows searching within the SNMP traps history, by this criterion:
   a. Search by hosts, metrics, MIB name, output and severity.

b. Search by status – Ok/Warning/Critical/Unknown.

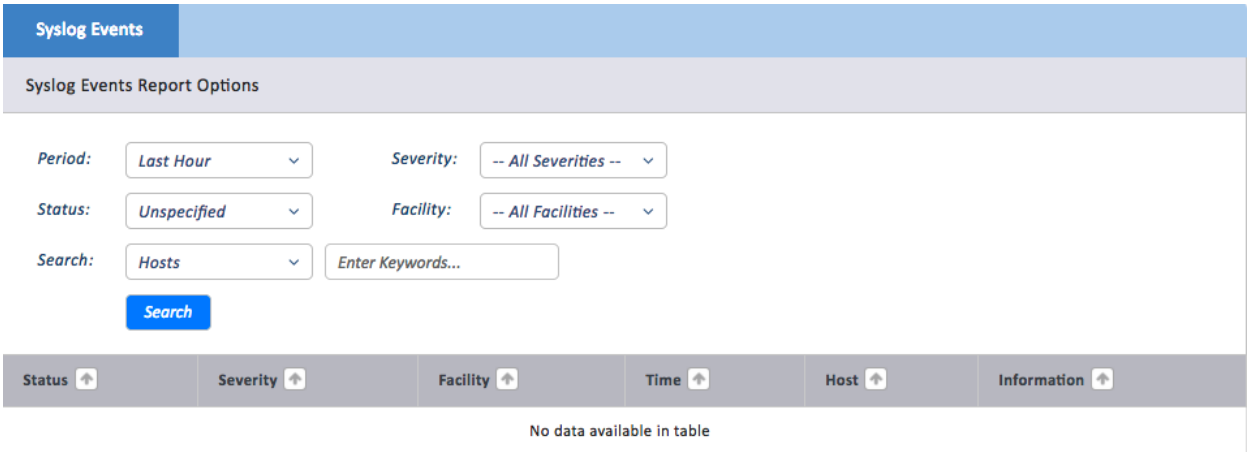
c. Search by keywords

2. **Report Time-Period**: What Schedule Time-Period the report is created for.
Click "**Search**" to display the report.



10.1.7 Syslog Report

Syslog Report Displays all syslog history and allows search and log filtering within the history.



1. **Search**: Allows searching within the syslog history, by this criterion:

a. Search by hosts, metrics and output.

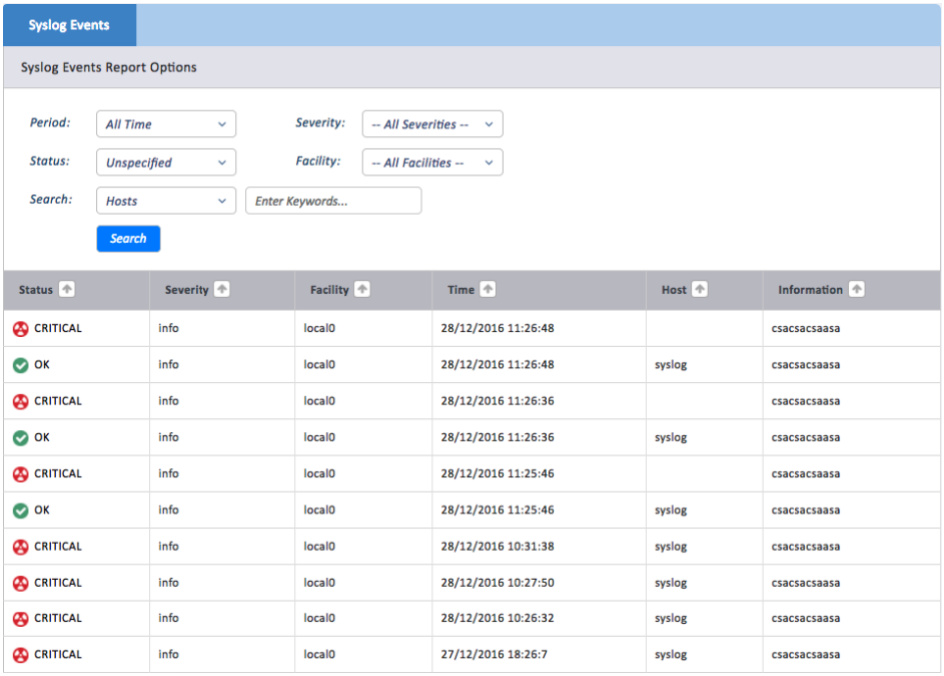
b. Search by status – Ok/Warning/Critical/Unknown.

c. Search by keywords

d. Search by syslog facility.

e. Search by severities – critical/alert/debug etc.

2. **Report Time-Period**: What Schedule Time Period the report is created for. Click "Search" to display the report.



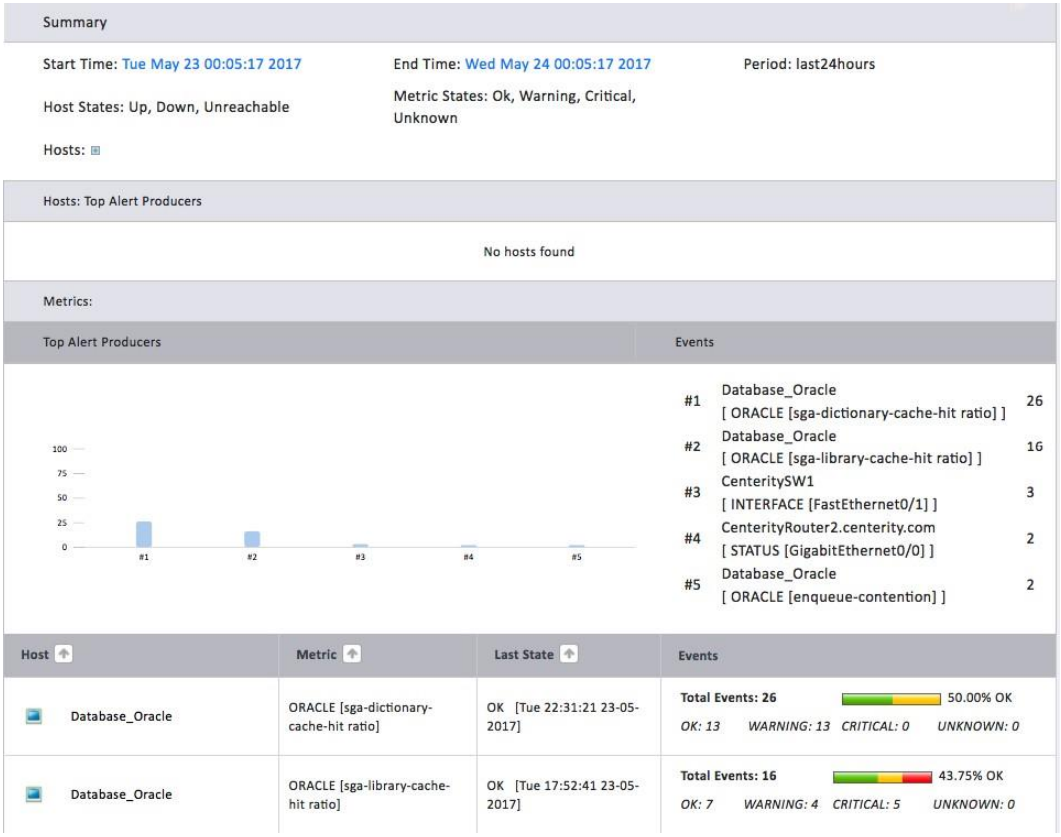
Status	Severity	Facility	Time	Host	Information
CRITICAL	info	local0	28/12/2016 11:26:48		csacsacsaasa
OK	info	local0	28/12/2016 11:26:48	syslog	csacsacsaasa
CRITICAL	info	local0	28/12/2016 11:26:36		csacsacsaasa
OK	info	local0	28/12/2016 11:26:36	syslog	csacsacsaasa
CRITICAL	info	local0	28/12/2016 11:25:46		csacsacsaasa
OK	info	local0	28/12/2016 11:25:46	syslog	csacsacsaasa
CRITICAL	info	local0	28/12/2016 10:31:38	syslog	csacsacsaasa
CRITICAL	info	local0	28/12/2016 10:27:50	syslog	csacsacsaasa
CRITICAL	info	local0	28/12/2016 10:26:32	syslog	csacsacsaasa
CRITICAL	info	local0	27/12/2016 18:26:7	syslog	csacsacsaasa

10.1.8 Summary Report

Generic reports about host and metric alert data, including alert totals, top alert producers, etc.

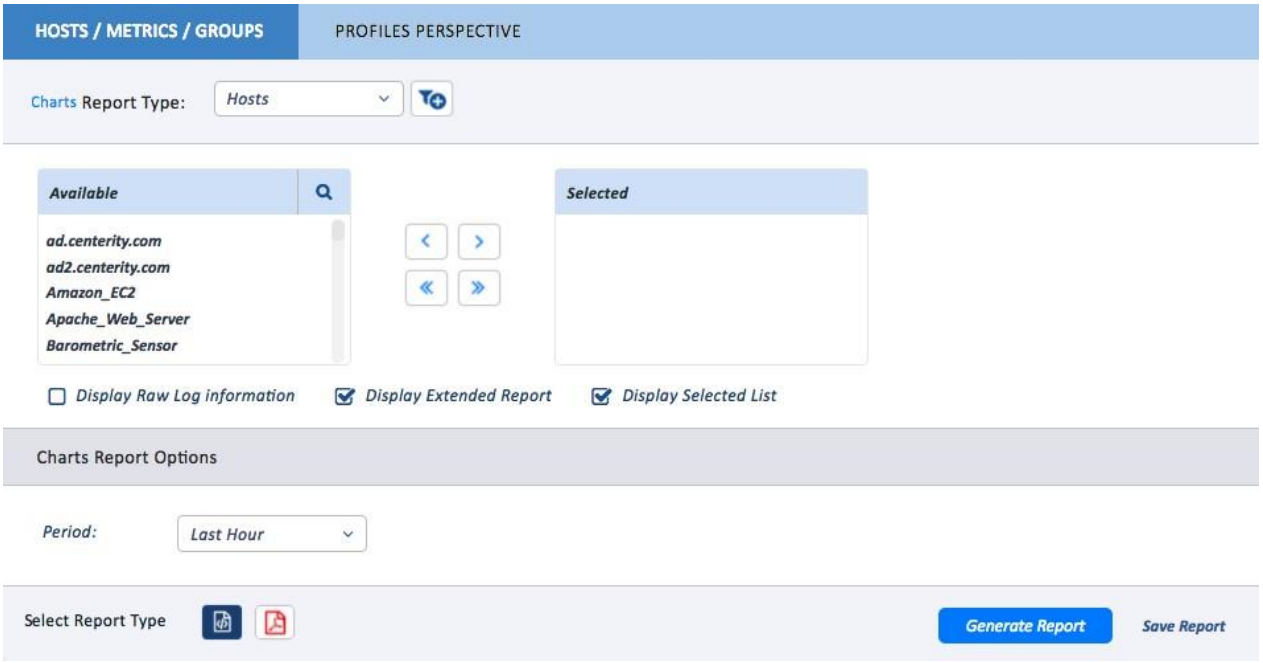
1. Report Types:
   a. **Standard report** - Uses all hosts.
   b. **Custom report** – Customize hosts.
2. **Report Period**: Choose from a set of predefined report periods or choose “CUSTOM REPORT PERIOD” and specify Start and End date.
   a. Start Date (Inclusive): Specify Start Date if “CUSTOM REPORT PERIOD” was selected.
   b. End Date (Inclusive): Specify End Date if “CUSTOM REPORT PERIOD” was selected.

3. **Top Alerters**: Choose the report:
   a. Top alert producers – Displays top 10 alert producers.
   b. Less alert producers – Displays bottom 10 alert producers.
   c. Most recent alerts – Displays most recent alerts.
4. **Report Type**: Display host alerts or metric alerts.
5. **Number of alerts**: The limit of alerts to display.

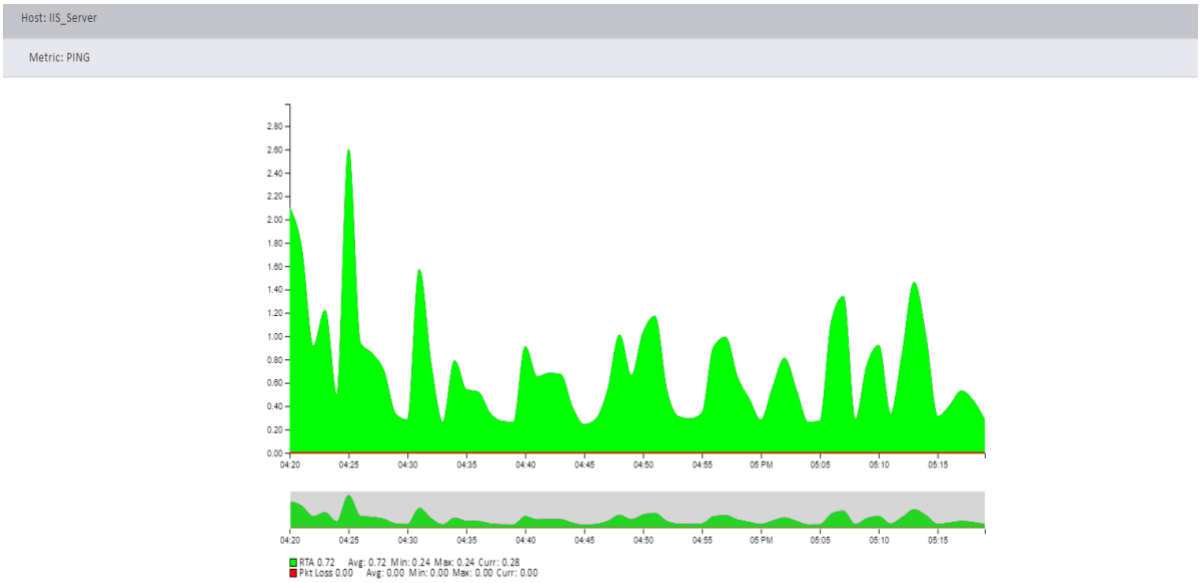


10.1.9 Charts Report

Charts report can display graph history in a selected time-period.

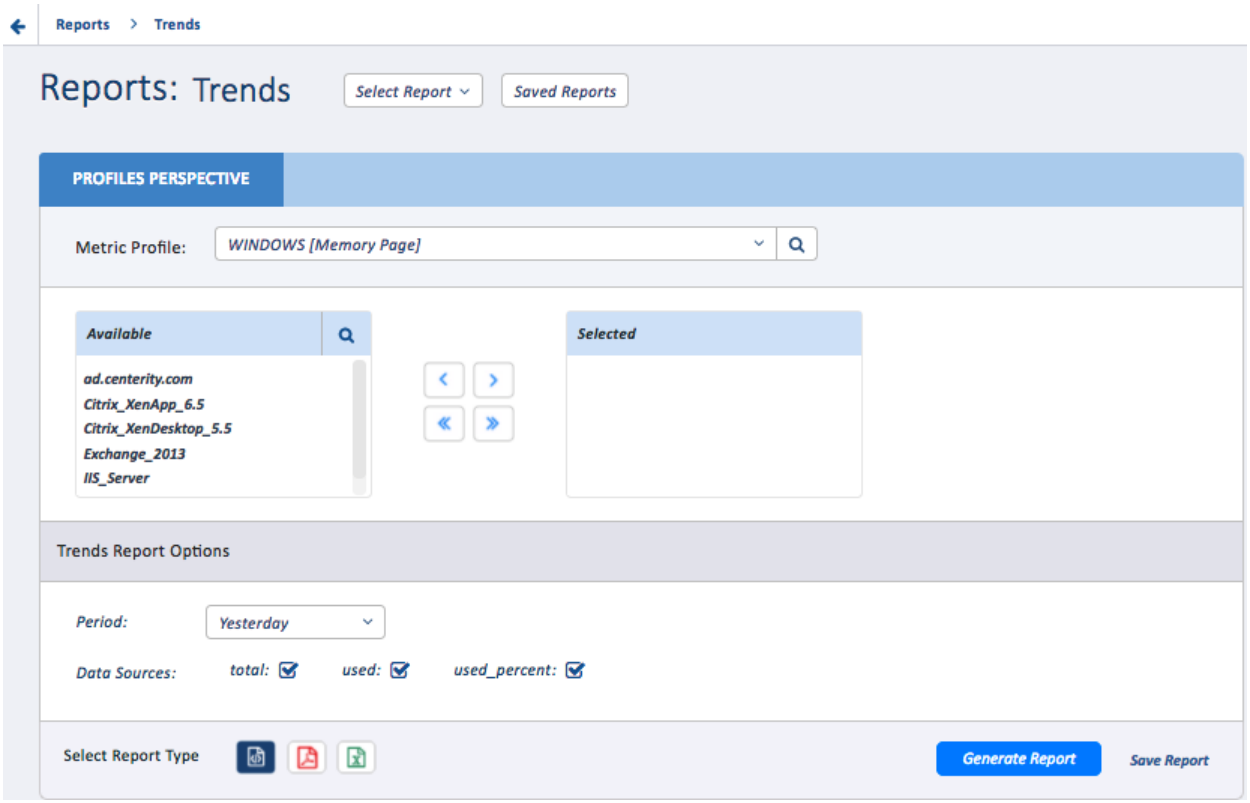


1. **Perspective type** - there are 4 options for this report. In each one - select the object from the left box and use the arrow to move into the right box.
   a. **Host / Metric /Group**:
      i. Host/Hosts graphs
      ii. Metric/Metrics graphs
      iii. Host group graphs
      iv. Business Service graphs (BSM)
   b. **Profile Perspective**: Allows availability by selected metric profile:
      i. Metric: Displays the metric profile within hosts.
      ii. BSM: Displays the metric profile within business services.
   c. **Display Raw Log information**: Displays event history log.
   d. **Display Extended Report**: Displays time duration of downtime as well as availability percentage.
   e. **Display Selected List**: Display/Don't display the host list in a PDF export.
   f. **Report Period**: Choose from a set of predefined report periods or choose "CUSTOM REPORT PERIOD" and specify Start and End date.
      i. Start Date (Inclusive): Specify Start Date if "CUSTOM REPORT PERIOD" was selected.
      ii. End Date (Inclusive): Specify End Date if "CUSTOM REPORT PERIOD" was selected.



10.1.10 Trends Report

Trends report displays a top 10 list of metric alerts, and a graph that compares the same metric profile on different hosts.



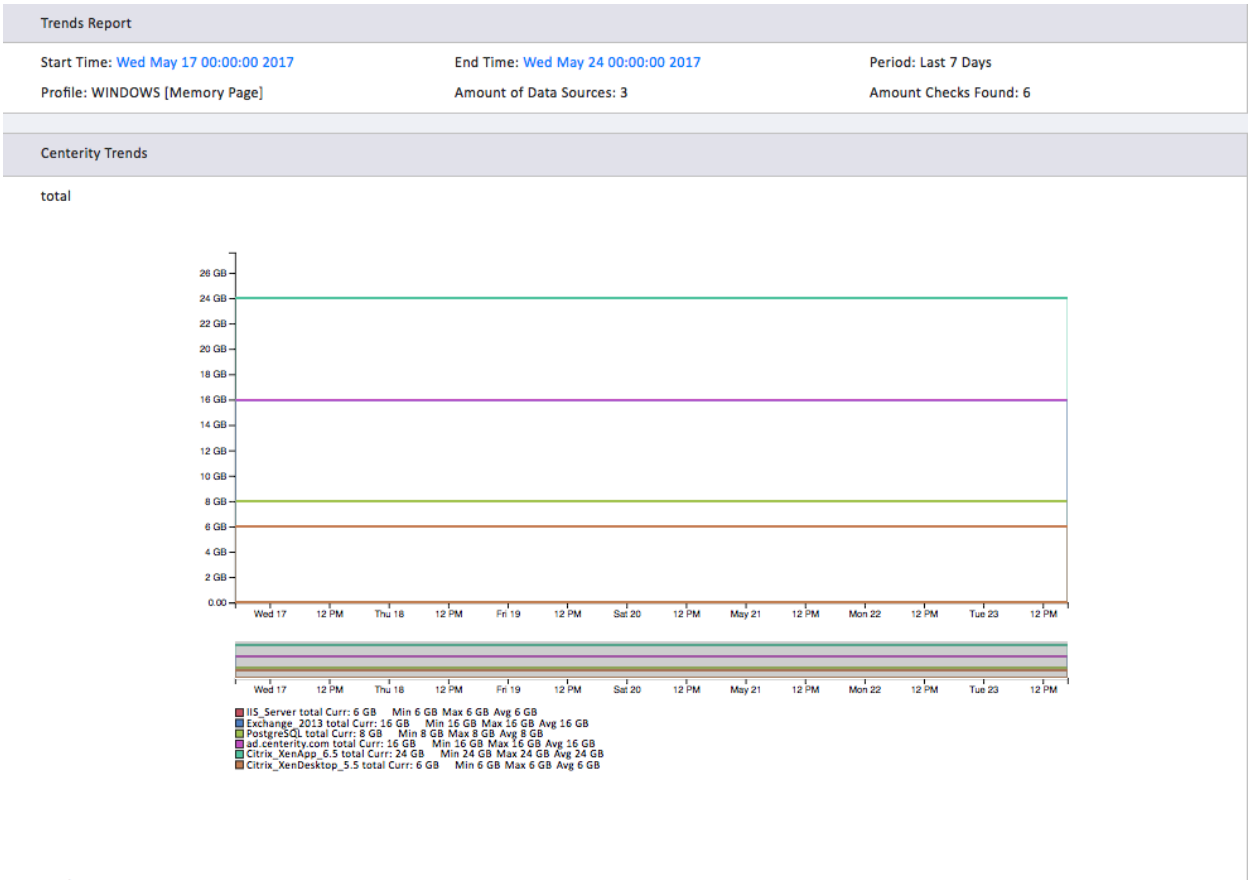
1. Select which Metric profile you wish to compare.
2. Select the hosts that monitor this metric profile.
3. Select various settings for your report:

a. Select **Data Sources**: This depends on the report analyzers for the metric, if there isn't an analyzer that fits this metric check, no data sources will appear, and you will not be able to generate a report.

b. **Report Period**: Choose from a set of predefined report periods or choose “CUSTOM REPORT PERIOD” and specify Start and End date.

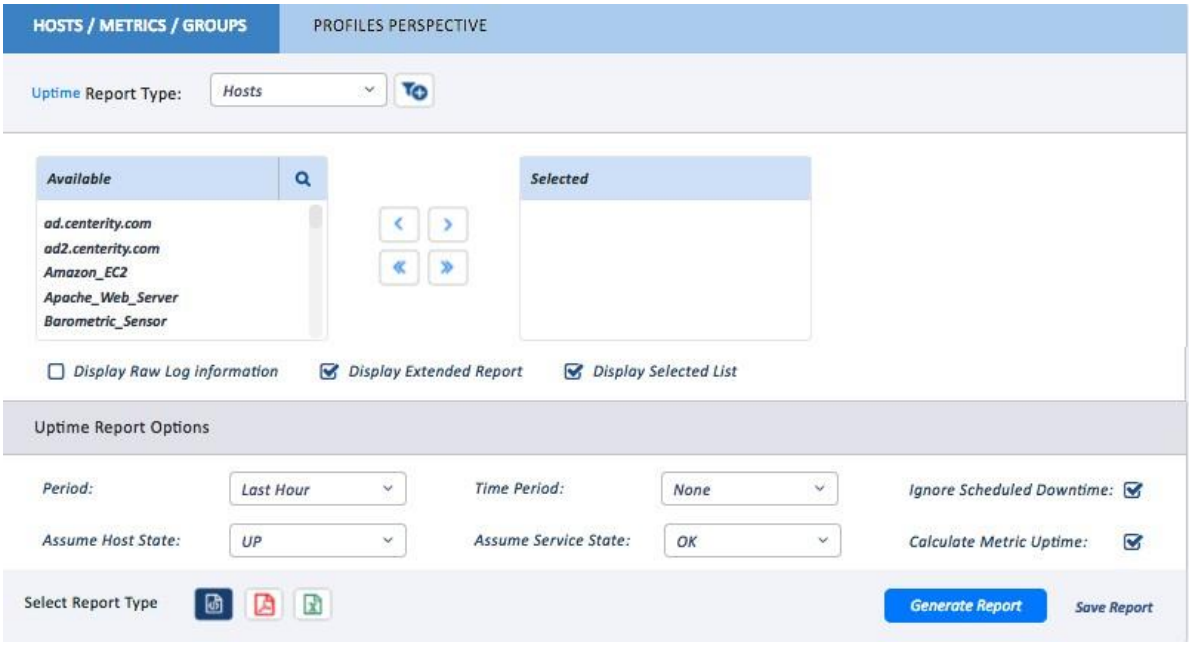
   i. Start Date: Specify Start Date if “CUSTOM REPORT PERIOD” was selected above.

   ii. End Date: Specify End Date if “CUSTOM REPORT PERIOD” was selected above.



10.1.11 Uptime Report

Shows the uptime of host groups, metric groups, hosts and metrics during a selected period of time.



1. **Perspective type** - there are 4 options for this report. In each one - select the object from the left box and use the arrow to move into the right box.
   a. **Host / Metric /Group**:
      i. Host/Hosts uptime
      ii. Metric / Metrics uptime
      iii. Host group uptime
      iv. Business Services uptime (BSM)
   b. **Profile Perspective**: Allows uptime by selected Metric profile:
      i. Metric: Displays the Metric profile within hosts.
      ii. BSM: Displays the Metric profile within business services.
   c. **Display Raw Log information**: Displays event history log.
   d. **Display Extended Report**: Displays time duration of downtime as well as availability percentage.
   e. **Display Selected List**: Display/Don't display the host list in a PDF export.
2. **Uptime Report Options**:
   a. **Report Period**: Choose from a set of predefined report periods or choose "CUSTOM REPORT PERIOD" and specify Start and End date.
      i. Start Date (Inclusive): Specify Start Date if "CUSTOM REPORT PERIOD" was selected.
      ii. End Date (Inclusive): Specify End Date if "CUSTOM REPORT PERIOD" was selected.

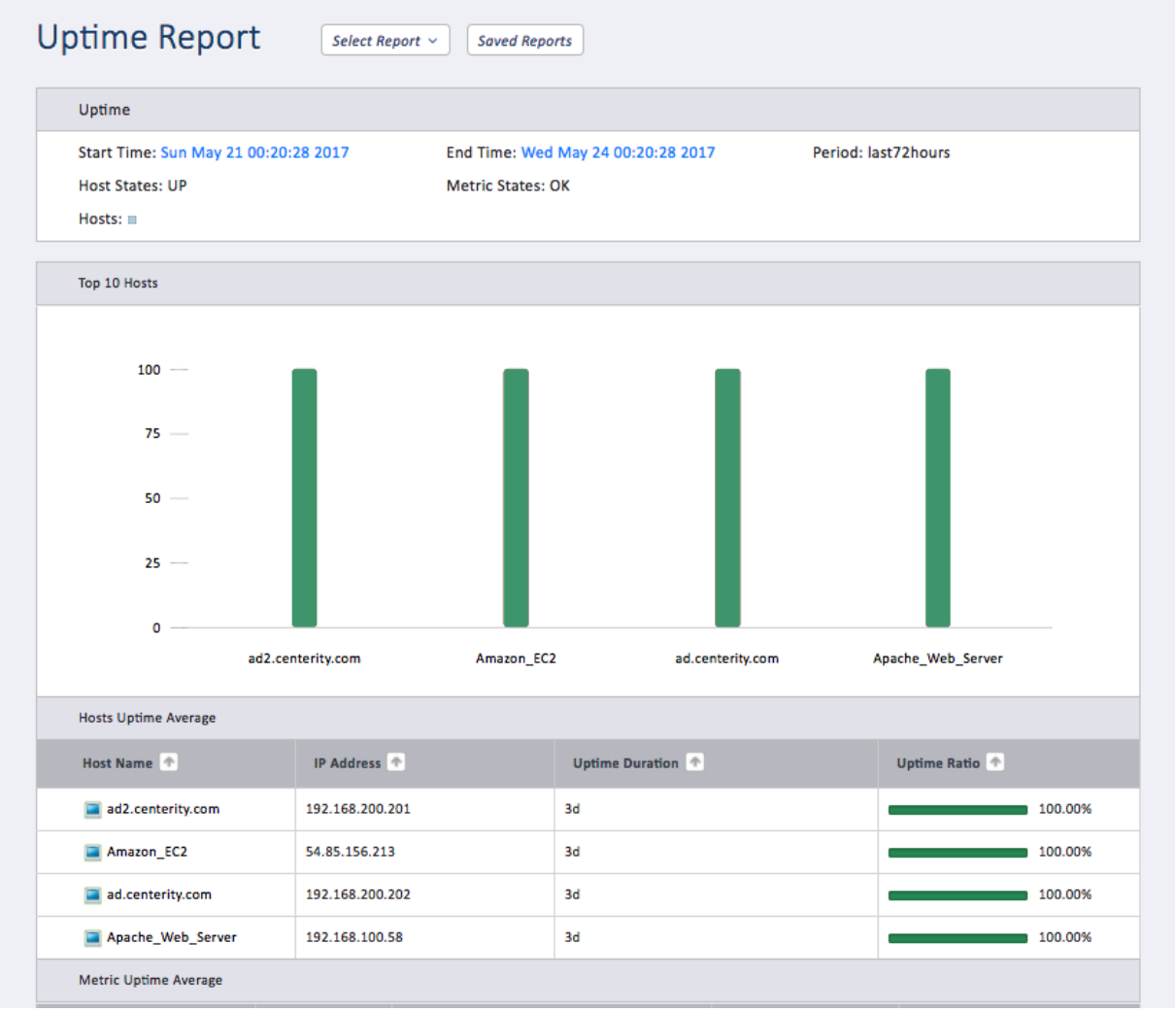
b. **Report Time Period**: What Schedule Time Period the report is created for.

c. **Ignore Scheduled Downtime**: The report will ignore any scheduled downtime on the host/ metric.

d. **Calculate Metric Uptime**: The report will display current uptime for this host.

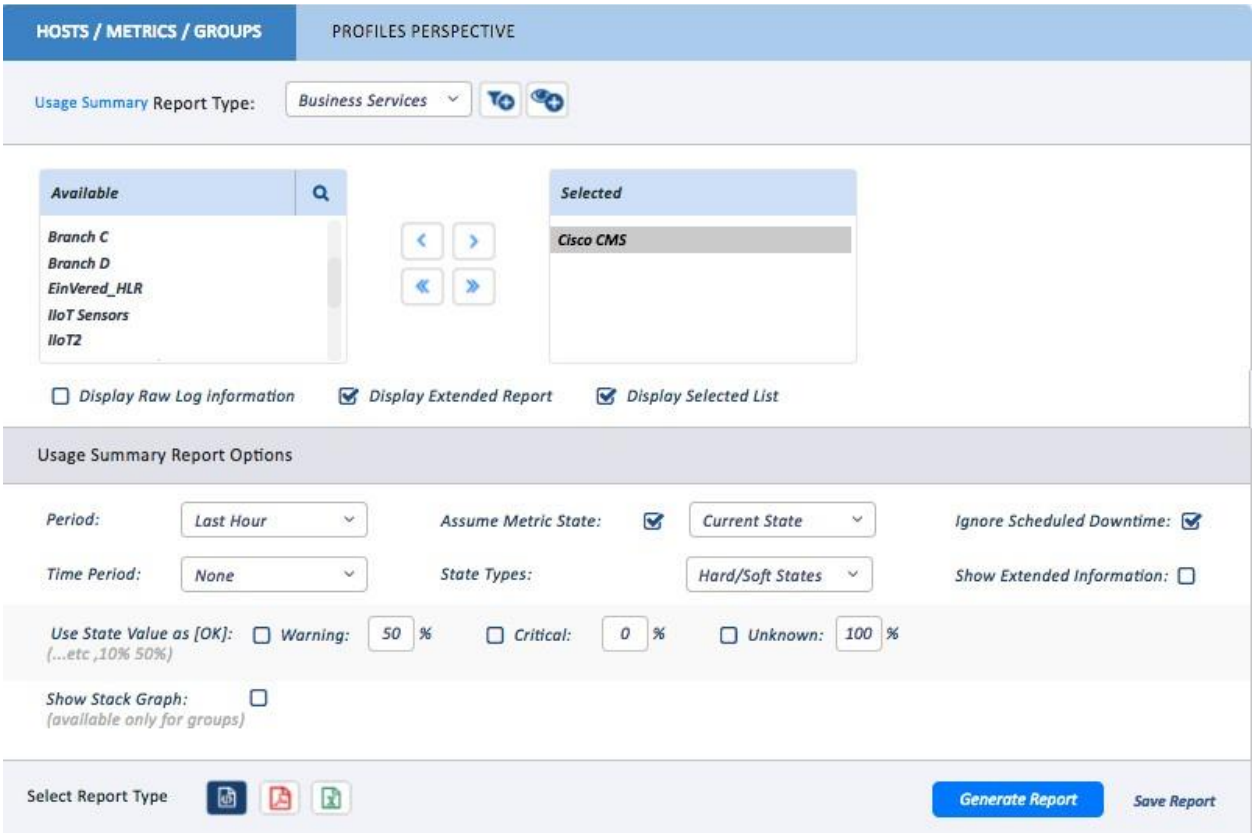
e. **Assumed Initial Host State**: If there is no information about the host or metric in the current log file, Centerity Monitor can assume status of the host. Default value is "UP".

f. **Assume Metric State**: If there is no information about the host or metric in the current log file, Centerity Monitor can assume status of the metric. Default value is "OK".



10.1.12 Usage Summary Report

This report is recommended for Metric groups (BSMs), it displays all usage summary for each Metric group divided to Level, and it displays all level failures and their effect on the other levels in the Metric group.



1. **Perspective type** - there are 4 options for this report. In each one - select the object from the left box and use the arrow to move into the right box.
   a. **Host / Metric /Group**:
      i. Metric / Metrics summary
      ii. Business Service summary (BSM)
   b. **Profile Perspective**: Allows availability by selected Metric profile:
      i. Metric: Displays the metric profile within hosts.
      ii. Metric Group: Displays the metric profile within business services.
   c. **Display Raw Log information**: Displays event history log.
   d. **Display Extended Report**: Displays time duration of downtime as well as availability percentage.
   e. **Display Selected List**: Display/Don't display the host list in a PDF export.
2. Select the Metric or Metric Group for the report.
   a. Select various settings for your report.

b. **Report Period**: Choose from a set of predefined report periods or choose "CUSTOM REPORT PERIOD" and specify Start and End date.

c. Start Date (Inclusive): Specify Start Date if "CUSTOM REPORT PERIOD" was selected above.

d. End Date (Inclusive): Specify End Date if "CUSTOM REPORT PERIOD" was selected above.

e. **Report Time Period**: What Schedule Time Period the report is created for.

f. **Ignore Scheduled Downtime**: The report will ignore any scheduled downtime on the host/ metric.

g. **Show Extended Information**: Gives a more detailed report, with smaller time period statistics.

h. **Show Stack Graph**: Displays a stack for each part of the chosen business services (available only for business services).

3. Use State Value as [Ok]: Choose thresholds to be stated ok in the report. The defaults are:

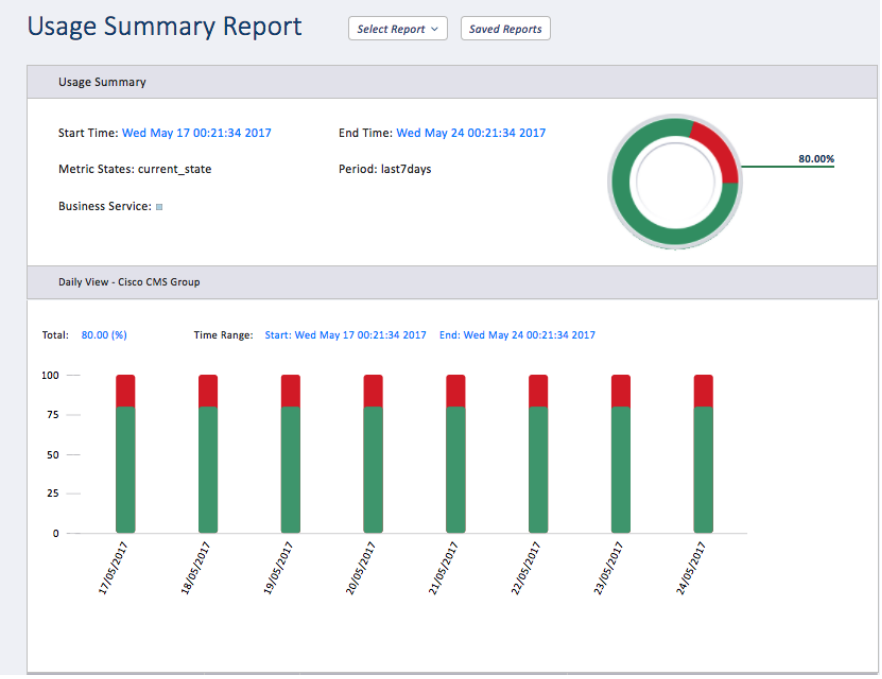
   a. Warning – 50 (Treat soft warning events as Ok).

   b. Critical - 0 (treat all critical events as critical).

   c. Unknown – 100 (Treat all unknown events as Ok).

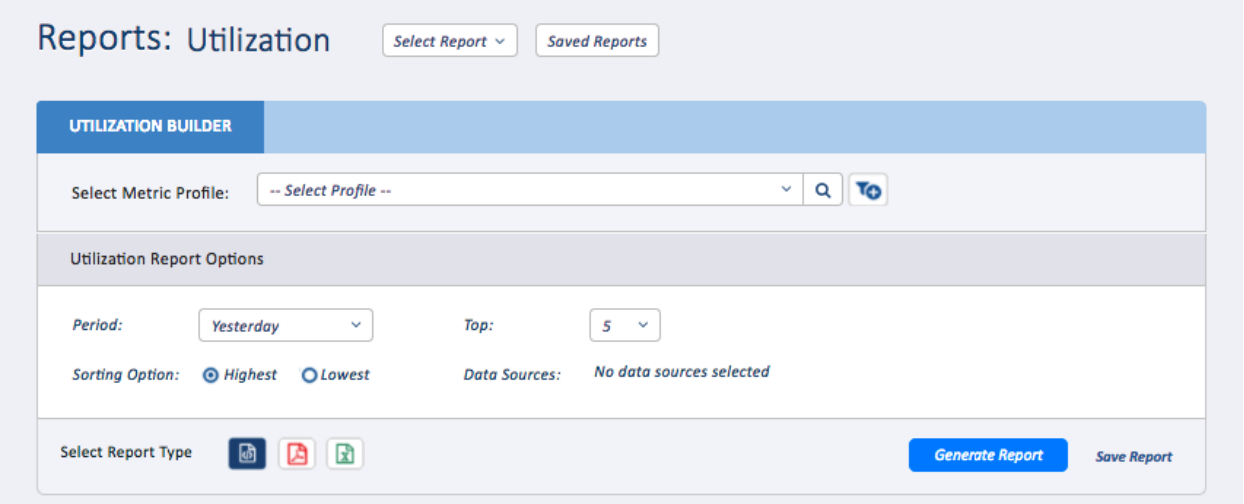
4. **Assume Metric State**: If there is no information about the host or metric in the current log file, Centerity Monitor can assume status of the host/metric. Default value is "Current State".

5. **State Type**: A problem is classified as a SOFT problem until the number of checks has reached the configured max check attempts value (Default: 3). When max check attempts are reached, the problem is reclassified as HARD and Centerity Monitor will send out a notification about the problem. SOFT problems do not result in notifications.

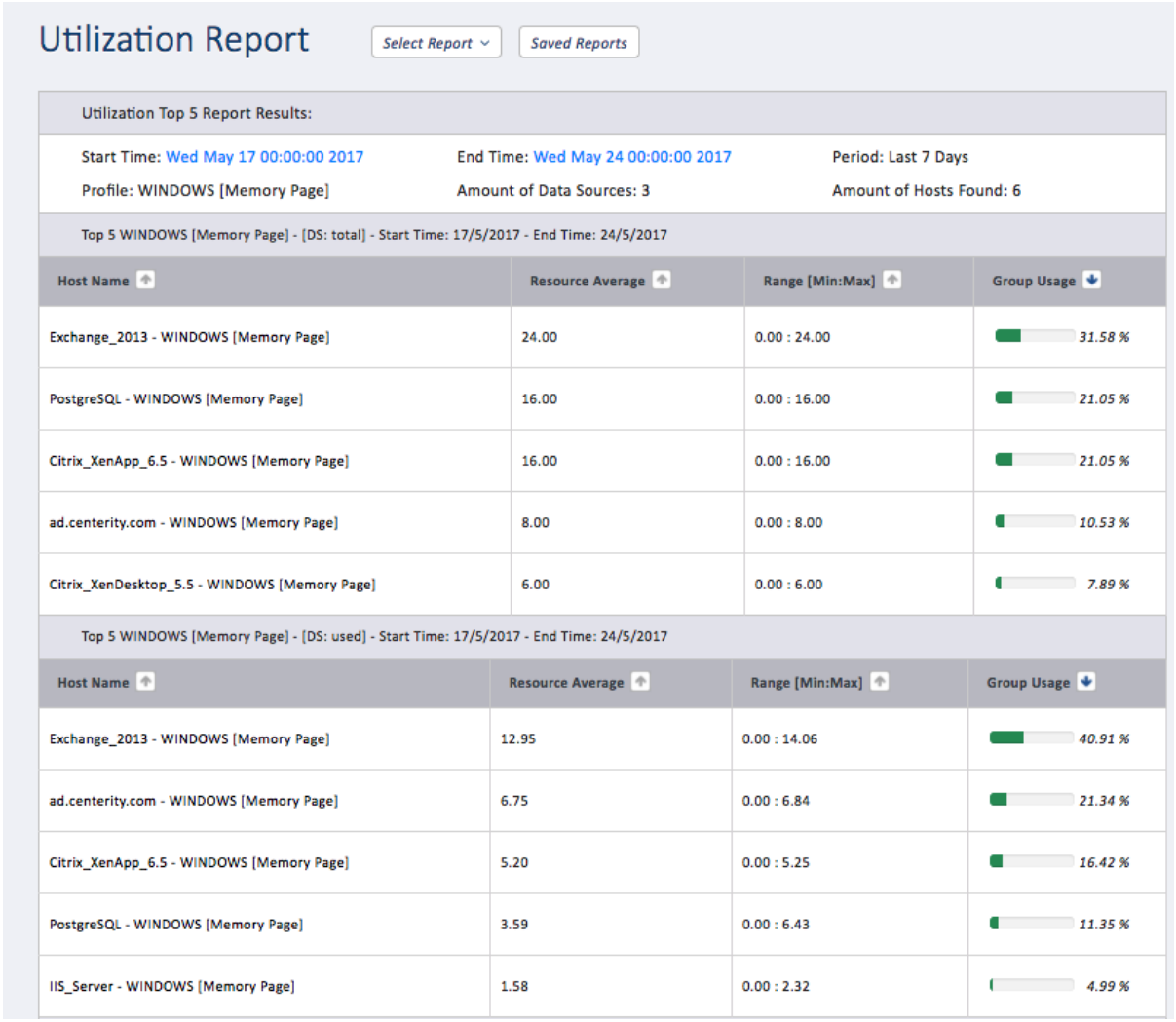


10.1.13 Utilization Report

Shows top 10 highest/lowest alerts producers.



1. Select the metric template for the report.
2. Select if highest or lowest values, and how many hosts to display – 5, 10, 15, etc.
3. Select various settings for your report:
   a. **Select Data Sources**: This depends on the report analyzers for the metric, if there isn't an analyzer that fits this metric check, no data sources will appear, but you can still generate the report.
   b. **Report Period**: Choose from a set of predefined report periods or choose “CUSTOM REPORT PERIOD” and specify Start and End date.
      i. Start Date (Inclusive): Specify Start Date if “CUSTOM REPORT PERIOD” was selected above.
      ii. End Date (Inclusive): Specify End Date if “CUSTOM REPORT PERIOD” was selected above.



Utilization Report

Select Report | Saved Reports

Utilization Top 5 Report Results:

Start Time: Wed May 17 00:00:00 2017 | End Time: Wed May 24 00:00:00 2017 | Period: Last 7 Days

Profile: WINDOWS [Memory Page] | Amount of Data Sources: 3 | Amount of Hosts Found: 6

Top 5 WINDOWS [Memory Page] - [DS: total] - Start Time: 17/5/2017 - End Time: 24/5/2017

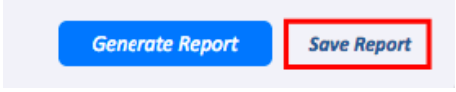
Host Name	Resource Average	Range [Min:Max]	Group Usage
Exchange_2013 - WINDOWS [Memory Page]	24.00	0.00 : 24.00	31.58 %
PostgreSQL - WINDOWS [Memory Page]	16.00	0.00 : 16.00	21.05 %
Citrix_XenApp_6.5 - WINDOWS [Memory Page]	16.00	0.00 : 16.00	21.05 %
ad.centerity.com - WINDOWS [Memory Page]	8.00	0.00 : 8.00	10.53 %
Citrix_XenDesktop_5.5 - WINDOWS [Memory Page]	6.00	0.00 : 6.00	7.89 %

Top 5 WINDOWS [Memory Page] - [DS: used] - Start Time: 17/5/2017 - End Time: 24/5/2017

Host Name	Resource Average	Range [Min:Max]	Group Usage
Exchange_2013 - WINDOWS [Memory Page]	12.95	0.00 : 14.06	40.91 %
ad.centerity.com - WINDOWS [Memory Page]	6.75	0.00 : 6.84	21.34 %
Citrix_XenApp_6.5 - WINDOWS [Memory Page]	5.20	0.00 : 5.25	16.42 %
PostgreSQL - WINDOWS [Memory Page]	3.59	0.00 : 6.43	11.35 %
IIS_Server - WINDOWS [Memory Page]	1.58	0.00 : 2.32	4.99 %

10.2 Creating a New Report Template

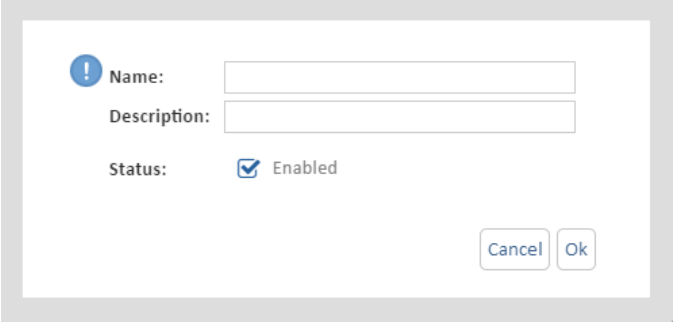
1. Select from the main menu Monitor➔ Reports view, and select the desired report.
2. Fill the required parameters for the report.
3. Click the “Save report” Button at the bottom-right pan



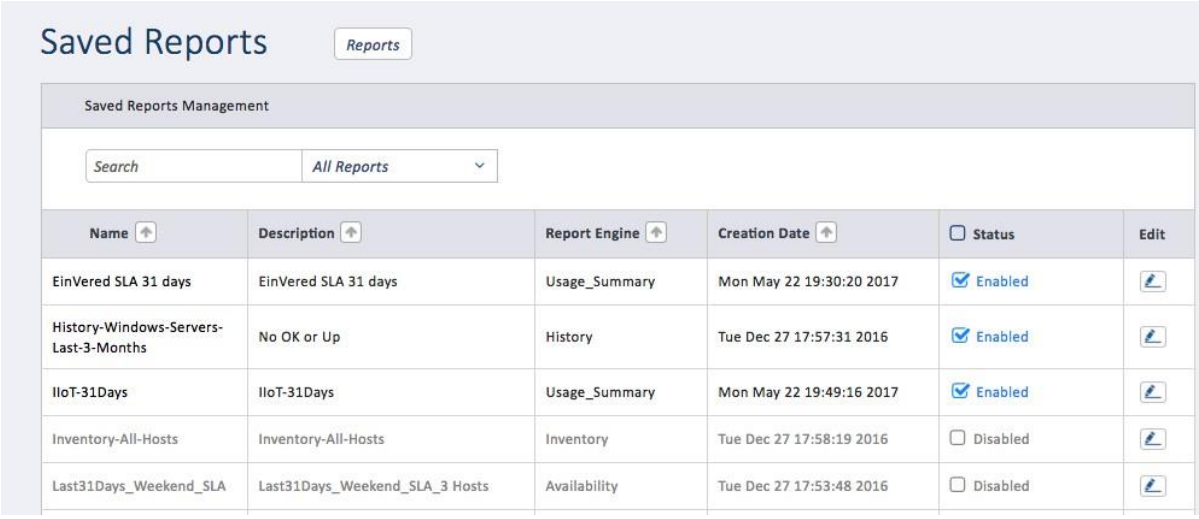
4. A popup window will be opened at the center of the screen. Fill the required p a r a m e t e r s :

a. Report-Name

b. Description



5. All reports can be found under “Saved Reports” section:



Appendix A. Traffic Analyzer

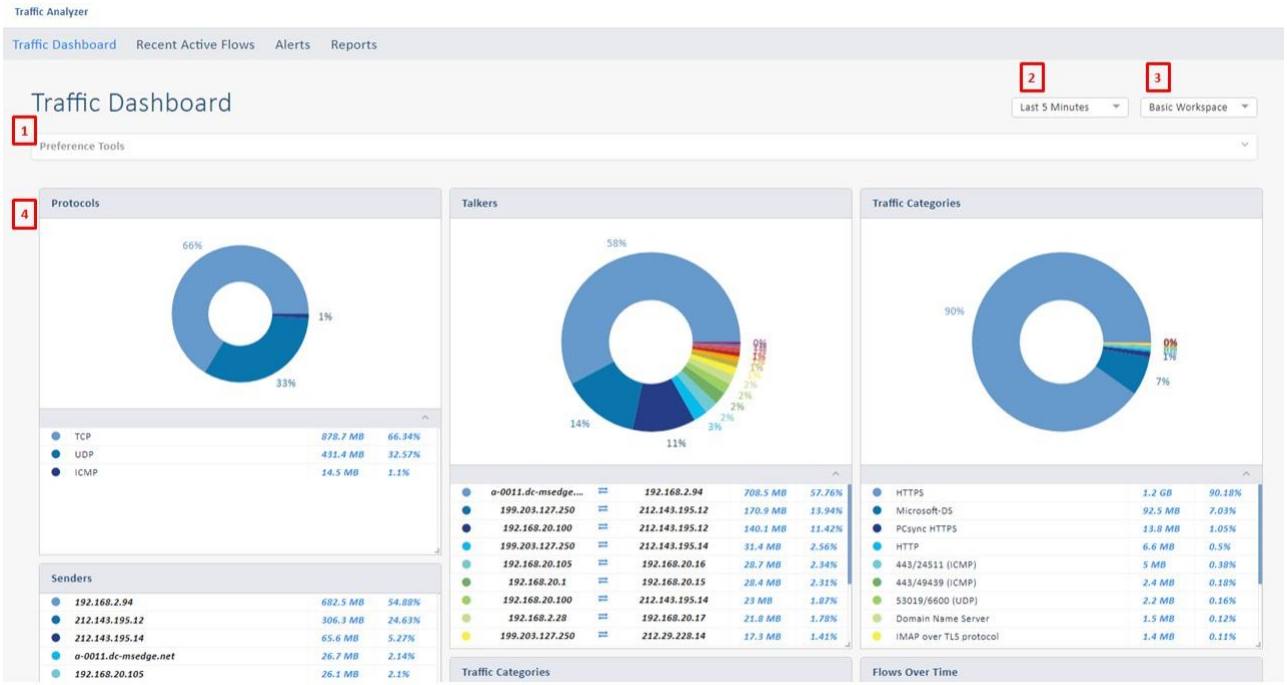
A.1 Using the Traffic Dashboard

Using the Traffic Dashboard panel, you can view site flow traffic detailed information and graphs. Configure your dashboard using preference tools. Preference tools are available for each type of analytics you monitor, including.

- Senders
- Receivers
- Talkers
- Protocols
- Groups
- Traffic Categories
- Traffic Sources
- Source Countries
- Destination Countries
- Flows Over Time

Each preference tool is configurable to display analytics as a pie chart and table data, table data only, or a bar chart only, as well as the number of top flows to display. Each user can configure Traffic Dashboards for individual requirements, save configurations, and switch between configurations to view flow information for different requirements at different times. Additionally, adjust the time frame of flows displaying in all preference tools.

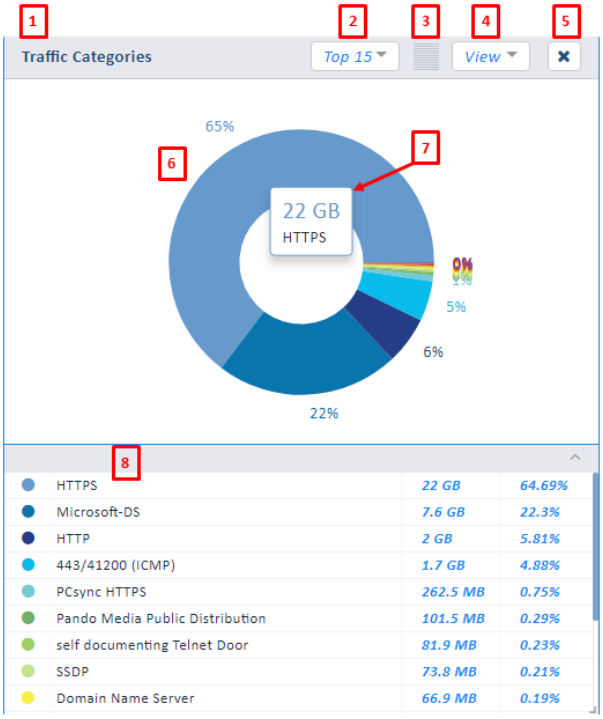
The following image and table describe the Traffic Dashboard panel.



#	Item	Description
1	Preference Tools list	Add, remove, and configure preference tools for flow analytics, including: ▪ **Senders** ▪ **Receivers** ▪ **Talkers** ▪ **Protocols** ▪ **Groups** ▪ **Traffic Categories** ▪ **Traffic Sources** ▪ **Source Countries** ▪ **Destination Countries** ▪ **Flows Over Time**
2	Flows Time frame list	Select the time frame of flows to display in all preference tools, including: ▪ **Last 5 Minutes** ▪ **Last 10 Minutes** ▪ **Last 15 Minutes** ▪ **Last Hour** ▪ **Last 2 Hours**

#	Item	Description
3	Workspace list	Manage your Traffic Dashboard workspace configuration, including: ▪ resetting your configuration to the basic view ▪ creating a new configuration ▪ using previous saved configurations ▪ deleting a configuration
4	Workspace	Area displaying your preference tools, including flow information and graphics.

This image and the following table describe a preference tool.



#	Item	Description
1	Preference tool name	The name of this preference tool.
2	Top flows list	The number of top flows to display, including: ▪ **Top 5** ▪ **Top 10** ▪ **Top 15**
3	Move	Drag and drop the preference tool on your Traffic Dashboard.

#	Item	Description
4	**View** list	The flow information analytics view, including: ▪ **Pie** - pie chart and table ▪ **Bar** - bar chart, only ▪ **Table** - table, only
5	✖	Remove the preference tool from the Traffic Dashboard.
6	Flow Analytics	The flow analytics information displayed in the format you select in the **View** list.
7	Detailed information	A balloon appearing when you hover over a chart segment containing details about that segment.
8	Flow	The table of flow information.

You can use IP addresses in preference tools as drill-downs to a Traffic Analyzer page containing detailed information for flows to that IP address.

A.1.1 Viewing the Traffic Dashboard

To view the Traffic Dashboard

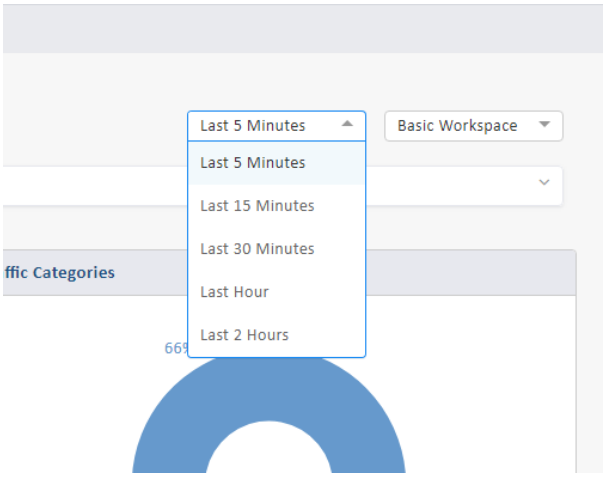
- In the Centerity Monitor menu, click Monitor and then, click **TRAFFIC ANALYZER**. The **Traffic Dashboard** panel appears.

A.1.2 Modifying the Recent Active Flows Time Frame

To modify the recent active flows time frame

- In the recent active flows list, select your required time frame, either:
  - **Last 5 Minutes**
  - **Last 10 Minutes**
  - **Last 15 Minutes**
  - **Last Hour**
  - **Last 2 Hours**

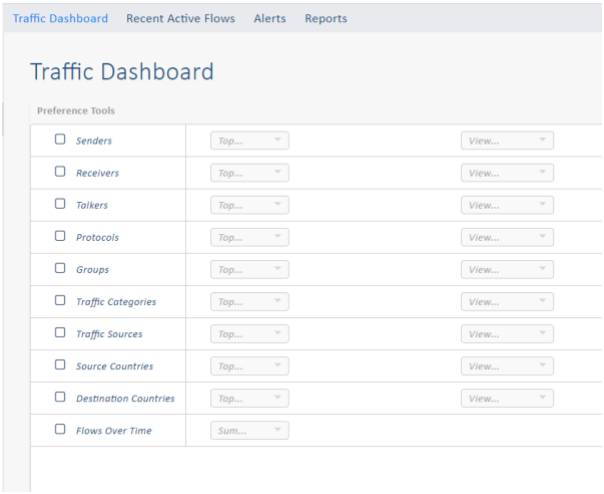
  Your **Traffic Dashboard** refreshes and the preference tools for your **Traffic Dashboard** configuration display flows for your required time frame.



A.1.3 Managing Preference Tools

You can add, modify, move, and remove Traffic Dashboard preference tools.

To add a preference tool to a Traffic Dashboard



1. On the **Preference Tools** list, select your required Preference Tool's check box, either:
   - **Senders**
   - **Receivers**
   - **Talkers**
   - **Protocols**
   - **Groups**
   - **Traffic Categories**
   - **Traffic Sources**
   - **Source Countries**
   - **Destination Countries**
   - **Flows Over Time**
2. On the **Top** list, select the number of top flows to view, either:
   - **Top 5**
   - **Top 10**
   - **Top 15**
3. On the **View** list, select the flow information display format, either:
   - **Pie** - pie chart and table
   - **Bar** - bar chart, only
   - **Table** - table, only

You must select from both the **Top** list and the **View** list.

4. Click Save. Your **Traffic Dashboard** refreshes and your preference tool appears.

To modify a preference tool

1. Hover over your required preference tool. The preference options appear.
2. Modify either of the following:
   - On the **Top** list, select the number of top flows to view, either:
     - **Top 5**
     - **Top 10**
     - **Top 15**
   - On the **View** list, select the flow information display format, either:
     - **Pie**
     - **Bar**
     - **Table**
3. The preference tool refreshes.

To move a preference tool on your Traffic Dashboard

1. Hover over your required preference tool. The preference options appear.
2. Using , drag and drop the preference tool to its new position.

To remove a preference tool from your Traffic Dashboard

1. Hover over your required preference tool. The preference options appear.
2. Click . The preference tool is removed.

A.1.4 Creating a New Traffic Dashboard

You can create a new Traffic Dashboard using your required recent active flows time frame and any combination of preference tools.

To create a new Traffic Dashboard

1. In the workspace list, click **New Workspace**.
2. In the **New Workspace** window, in the **Workspace Name** text box, type your new Traffic Analyzer dashboard workspace name.

3. Configure your new Traffic Analyzer dashboard by doing the following:
   - Set your recent active flows time frame - see the instructions in To modify the recent active flows time frame
   - Add your preference tools - see the instructions in To add a preference tool to a Traffic Dashboard.

You can also modify, move, and remove your preference tools, see the instructions in:

- To modify a preference tool
- To move a preference tool on your Traffic Dashboard
- To remove a preference tool from your Traffic Dashboard.

A.1.5 Switching Traffic Dashboards

You can switch between your saved Traffic Dashboard and view traffic analytics for various requirements.

To switch Traffic Dashboard configurations

- In the workspace list, click the name of your required Traffic Dashboard configuration. The Traffic Dashboard refreshes and the named Traffic Dashboard configuration appears.

A.1.6 Deleting a Traffic Dashboard

You can delete a Traffic Dashboard.

To delete a Traffic Dashboard

1. In the Traffic Dashboard list, click **Delete Workspace**.
2. In the Delete Workspace window, in the workspace name list, click your required workspace name.
3. Click

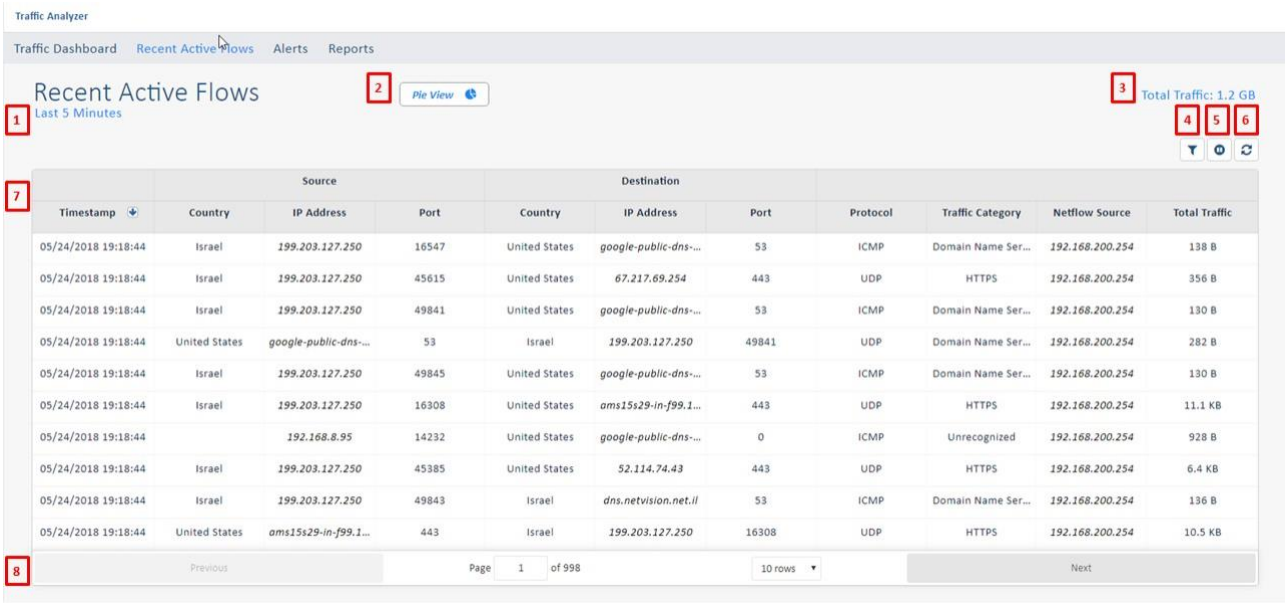
. Your Traffic Analyzer dashboard workspace is deleted.

A.2 Viewing Recent Active Flows

Using the Recent Active Flows panel, you can view total traffic for the recent active flows time frame, view, filter, and sort flow analytics, and view a pie chart configurable by protocol, talkers, and traffic for the top 5, 10, or 15 flows. Recent active flows are summarized by time and include the following analytics:

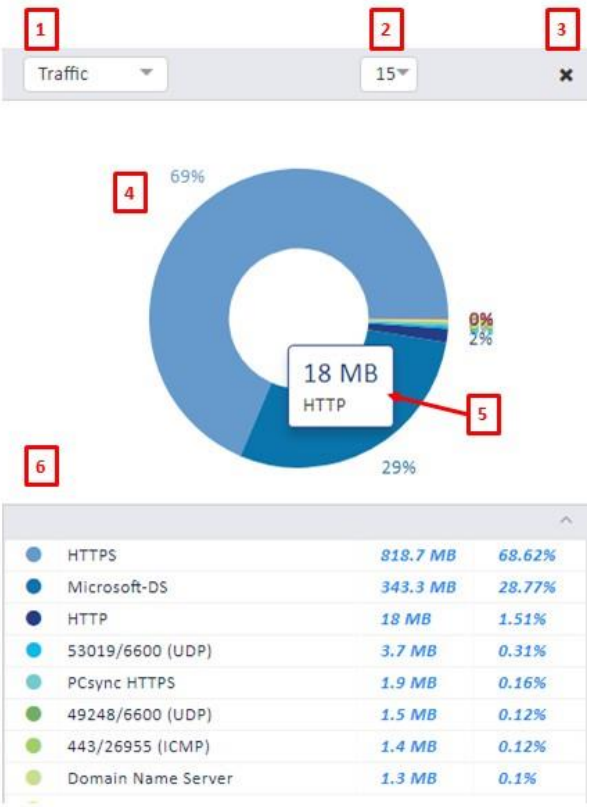
- Timestamp of the flow
- Source country
- Source IP address
- Source port
- Destination country
- Destination IP address
- Destination port
- Protocol
- Traffic category
- NetFlow source
- Total traffic for the flow

The following image and table describe the Recent Active Flows panel.



#	Item	Description
1	Time frame	The time frame of the recent active flows displayed. The time frame is set by your administrator.
2	Pie View	Displays a pie chart showing any of the following flows: ▪ Protocols ▪ Talkers ▪ Traffic
3	**Total Traffic**	The total traffic on recent active flows in the time frame.
4		Filter the recent active flows for any combination of the following fields: ▪ **Timestamp** ▪ **Source Country** ▪ **Source IP address** ▪ **Source port** ▪ **Destination country** ▪ **Destination IP address** ▪ **Destination port** ▪ **Protocol** ▪ **Traffic category** ▪ **Netflow Source**
5		Stop auto refresh of the alerts information. This can be useful to prevent flow analytics from updating while you are examining them.
6	Refresh	Refresh the recent active flow data.
7	Recent active flows	Workspace containing the recent active flows.
8	Navigation bar	Use to navigate the recent active flow data, including: ▪ **Previous** - display previous page of recent active flows ▪ Page number - use to move to a page number ▪ Rows - use to modify the number of rows displayed ▪ **Next** - display the next page This navigation bar also shows the total number of pages.

This image and the following table describe the Recent Active Flows pie chart.



#	Item	Description
1	Flows list	The recent active flow to display as a pie chart, including: ▪ **Protocols** ▪ **Talkers** ▪ **Traffic**
2	Top Flows Menu	The top recent active flows to display, including ▪ **5** - top 5 ▪ **10** - top 10 ▪ **15** - top 15
3	Close	Close the recent active flows pie chart.
4	Pie chart	A pie chart displaying the recent active flows for the flow and top flows selected.
5	Detailed information	A balloon appearing when you hover over a chart segment containing details about that segment.
6	Recent Active Flows	The recent active flows data for the flow and top flows selected.

A.2.1 Viewing Recent Active Flows

To view the recent active flows

1. In the Centerity Monitor menu, click Monitor and then, click **TRAFFIC ANALYZER**. The **Traffic Dashboard** panel appears.
2. Click the **Recent Active Flows** tab. The **Recent Active Flows** panel appears.

A.2.2 Managing Your Recent Active Flows View

To manage your recent active flows view

- In the **Recent Active Flows** panel, you can do any of the options described in the following table.

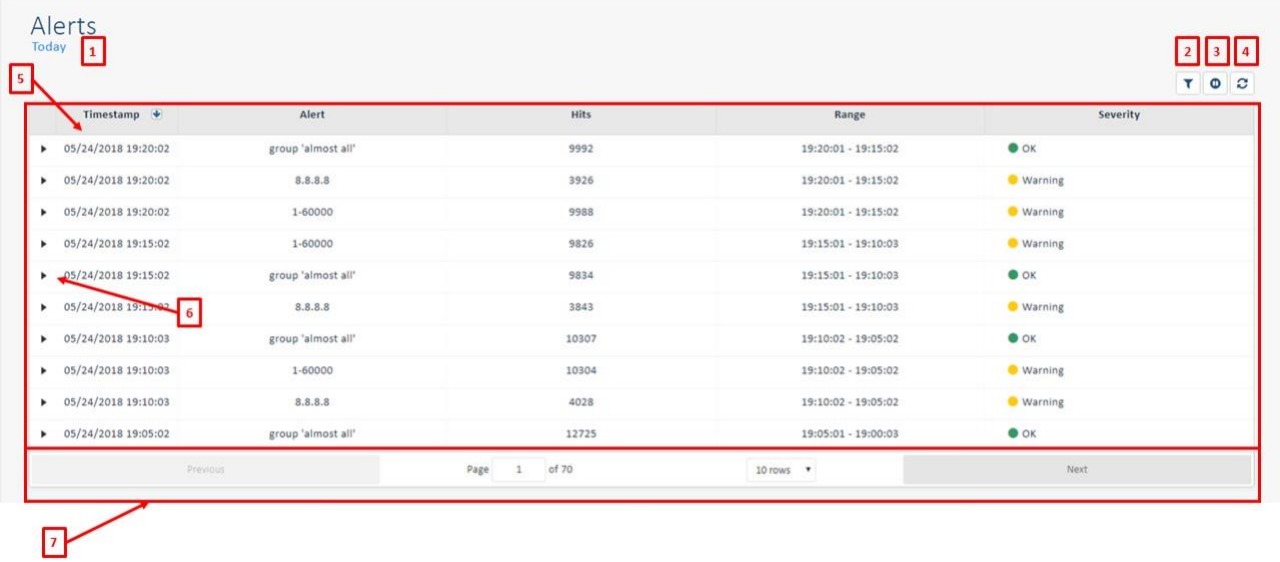
Option	Description
Sort	Click a column title.
	Click and in your required column filter, choose your required value. You can add more than one value for a filter.
	Click to stop auto refresh to prevent the recent active flows from updating while you view them.
	Click to refresh the recent active flows now (do not wait for the next recent active flows update).
Drill-down	In the **Recent Active Flows** workspace, in your required row, click any of the following specific row values: ▪ source IP address ▪ destination IP address ▪ NetFlow IP address A detailed flows page for that IP address appears.

You can also use the navigation bar to view other pages and modify the number of rows displayed on a page.

A.3 Viewing Alerts

Using the Alerts panel, you can view the alerts your organization defines for your contact group. Alerts are grouped by time frame, alert name, and severity. You can drill down into an alert group for details.

The following image and table describe the Alert panel.



#	Item	Description
1	Time frame	The time frame of the alerts displayed.
2		Filter the alerts table data for any of the following fields: ▪ Timestamp ▪ Alert name ▪ Severity
3		Stop auto refresh of the alerts information. This can be useful to prevent alerts from updating while you are examining them.
4		Refresh the alerts information now.
5	Alerts	The alert information containing summarized alert details.

#	Item	Description
6	▸	Expand the summarized alert and view the detailed alert information row.
7	Navigation bar	Use to navigate the recent active flow data, including: ▪ **Previous** - display previous page of recent active flows ▪ Page number - use to move to a page number ▪ Rows - use to modify the number of rows displayed ▪ **Next** - display the next page This navigation bar also shows the total number of pages.

A.3.1 Viewing Alerts

To view alerts

1. In the Centerity Monitor menu, click Monitor and then, click **TRAFFIC ANALYZER**. The **Traffic Dashboard** panel appears.
2. Click the **Alerts** tab. The **Alerts** panel appears.

A.3.2 Managing Your Alerts View

To manage your alerts view

- In the **Alerts** panel, you can do any of the options described in the following table.

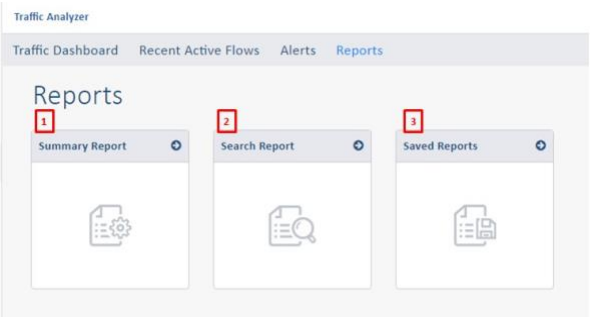
Option	Description
Sort	Click a column title.
	Click and in your required column filter, choose your required value. You can add more than one value for a filter.
	Stop auto refresh to prevent the alerts from updating while you view them.
	Refresh the alerts now (do not wait for the next recent active flows update).
Drill-down	Expand an alert row to view the individual alerts.

You can also use the navigation bar to view other pages and modify the number of rows displayed on a page.

A.4 Generating Reports

Using the Reports panel, you can generate and reuse saved analytics reports, including a summary report and search report. Use report filters, include graphics, save report settings for reuse, and export reports to PDF and Excel spreadsheet file from your reports.

This image and the following table describe the Reports panel.



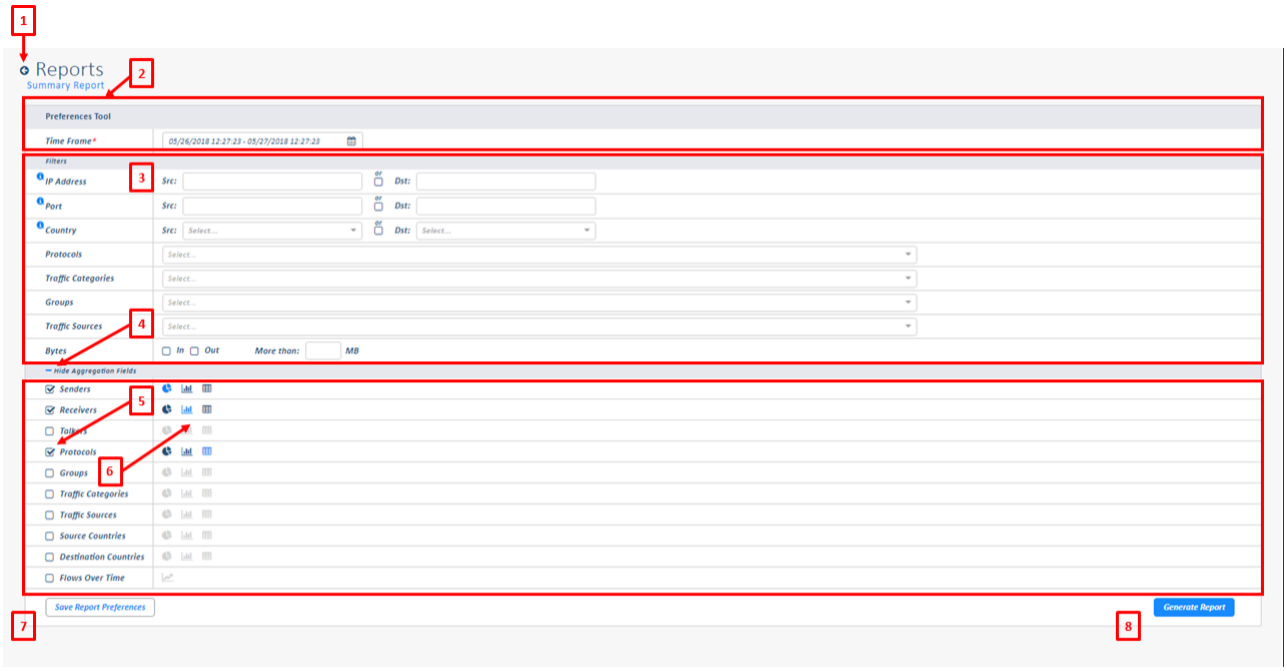
#	Item	Description
1	Summary Report	A report summarizing the total traffic over the time frame you specify, for the filters you select, and grouped by your selected object(s). Also include table data or a graph for aggregate fields. Aggregate fields are flow fields, including: ▪ **Senders** ▪ **Receivers** ▪ **Talkers** ▪ **Protocols** ▪ **Groups** ▪ **Traffic Categories** ▪ **Traffic Sources** ▪ **Source Countries** ▪ **Destination Countries** ▪ **Flows Over Time** For example, report total traffic for each protocol coming in and out for a specific port today, and include a bar chart of protocols as an aggregate field.
2	Search Report	A detailed report of all traffic over the time frame you specify, for the filters you select. For example, all traffic from a specific IP address to a specific IP address through a specific port today.
3	Saved Reports	Summary and detailed reports settings you name and save for reuse.

To view Reports

1. In the Centerity Monitor menu, click Monitor and then, click **TRAFFIC ANALYZER**. The **Traffic Dashboard** panel appears.
2. Click the **Reports** tab. The **Reports** panel appears.

A.4.1 Summary Report

The following image and table describe the Summary Reports panel.



#	Item	Description
1		Return to the Reports page.
2	Time Frame	The to/from date and time of flows to include in your summary report. The time frame includes: ▪ **Last 30 Minutes** ▪ **Last Hour** ▪ **Today** ▪ **Yesterday** ▪ **Last 7 Days** ▪ **Last 30 Days** ▪ **This Month** ▪ a custom time frame you select
3	Filters	The flows fields and the values you specify to include in your report.

#	Item	Description
4	Show/hide aggregation fields	Show/hide the aggregate fields pane.
5	Aggregation field check box	Select an aggregation field to include in your report, including: ▪ **Senders** ▪ **Receivers** ▪ **Talkers** ▪ **Protocols** ▪ **Groups** ▪ **Traffic Categories** ▪ **Traffic Sources** ▪ **Source Countries** ▪ **Destination Countries** ▪ **Flows Over Time**
6		Use to select the type of aggregation field chart to include in your summary report, including: ▪ Pie chart ▪ Bar chart ▪ Table
7		Use to save your summary report settings for reuse.
8		Use to create your summary report.

To generate a summary report

1. In the **Preference Tools** area, in **Time Frame**, choose your required time frame.
2. In the **Filters** area, select any of the following filters, its **Src** (source to include in the report), **Dst** (destination to include in the report), and select the **OR** check box to include filters matching either the source or destination (the default is "AND" to include both):
   - **IP Address**
   - **Port**
   - **Country**

You can add more than one IP address, Port, or Country by clicking additional list items.

3. In each of the following lists, select your required filters.
   - **Protocols**
   - **Traffic categories**
   - **Groups**
   - **Traffic Sources**
4. In **Bytes**, select the **In** (incoming) and/or **Out** (outgoing) check boxes and in **More than** type the minimum number of bytes incoming and/or outgoing to report.
5. If you require aggregate fields added to your report, do the following:
   a. Click + Show Aggregation Fields. The aggregate fields pane expands.
   b. For each aggregate field you require, select either Pie View (Pie Chart), (Bar Chart), or (Table).
6. Click Generate Report. Your summary report appears.

To save and reuse your report

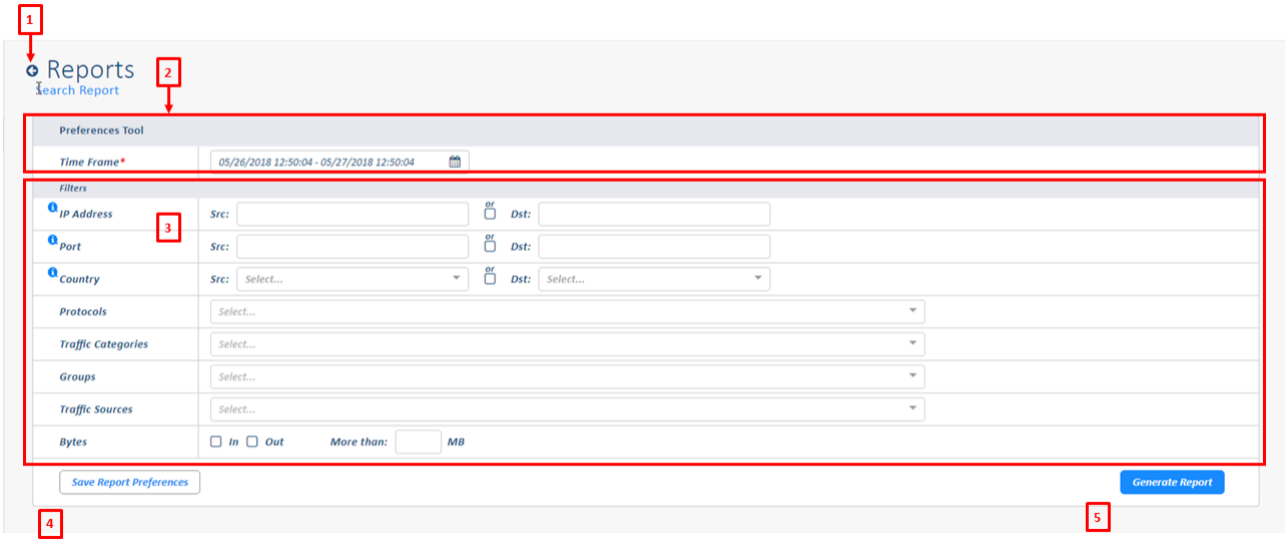
1. Click Save Report Preferences. The Save Report Preferences window appears.
2. In **Report Name**, type your report name, and then click **Save**. Your saved report is now available in **Saved Reports**.

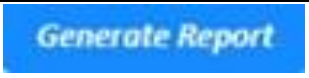
To export your report

- Click - a PDF file containing your report is downloaded.
- Click - an Excel file containing your report is downloaded.

A.4.2 Search Report

The following image and table describe the Search Report panel.



#	Item	Description
1		Return to the Reports page.
2	Time Frame	The to/from date and time of flows to include in your report. The time frame includes: ▪ **Last 30 Minutes** ▪ **Last Hour** ▪ **Today** ▪ **Yesterday** ▪ **Last 7 Days** ▪ **Last 30 Days** ▪ **This Month** ▪ a custom time frame you select.
3	Filters	Specify the flows to include in your summary report.
4		Save your summary report settings for reuse.
5		Create your summary report.

To generate a search report

1. In Traffic Analyzer, click the **Reports** tab. The Report panel appears.
2. Click **Search Report**. The Search Report panel appears.
3. In the **Preference Tools** area, in **Time Frame**, choose your required time frame.

4. In the **Filters** area, select any combination of the following filters:
   - **IP Address** - in **Src** and/or **Dst**, type your source and/or destination, respectively. Select the **OR** check box to include filters matching either. You can use a comma separated list of IP addresses and ranges.
   - **Port** - in **Src** and/or **Dst**, type your source and/or destination, respectively. Select the **OR** check box to include filters matching either. You can use a comma separated list of ports and ranges.
   - **Country** - in the **Src** list and/or and **Dst** list, choose your source and/or destination, respectively. Select the **OR** check box to include filters matching either. You can add more than one country.
   - **Protocols** - in the **Protocols** list, choose your required protocols.
   - **Traffic categories** - in the **Traffic categories** list, choose your required traffic categories.
   - **Groups** - in the **Groups** list, choose your required analytics groups.
   - **Traffic Sources** - in the **Groups** list, choose your required source devices.
   - **Bytes** - select the **In** (incoming) and/or **Out** (outgoing) check boxes and in **More than:** type the minimum number of bytes incoming and/or outgoing to report.
5. Click Generate Report. Your summary report appears.

To save and reuse your report

1. Click Save Report Preferences. The Save Report Preferences window appears.
2. In **Report Name**, type your report name, and then click **Save**. Your saved report is now available in **Saved Reports**.

To export your report

- Click - a PDF file containing your report is downloaded.
- Click - an Excel file containing your report is downloaded.

A.4.3 Saved Reports

Using saved reports, you can do any of the following:

- generate a report using saved report filters
- edit saved report filters
- create a new saved report from edited filters
- delete a saved report

To generate a report using saved report filters, edit saved report filters, or create a new saved report from edited filters

1. In Traffic Analyzer, click the **Reports** tab. The Report panel appears.
2. Click **Saved Reports**.
3. In the saved report list, in your required saved report row, either:
   - Click your required saved report name.
   - Click .

   The report filters page appears.
4. If required, edit any combination of the filters.
5. Do any of the following:
   - Generate your saved report - Click .

To export your report

- Click - a PDF file containing your report is downloaded.
- Click - an Excel file containing your report is downloaded.

   - Update your saved report's filter - Click .
   - Create a new saved report - Click .

To delete a saved reports(s)

1. In the saved report list, select the check box(es) of the saved reports to delete.
2. Click .
3. Click . Your saved reports are deleted.