Videoscape Distribution Suite Service Manager User Guide

First Published: August 03, 2012

Last Modified: July 19, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-29472-01

VDS Service Manager Analytics and Provisioning Portal User Guide

CONTENTS

Preface

Audience

The Videoscape Distribution Suite Service Manager (VDS-SM) User Guide provides instructions to the Operators and Administrators, who are responsible for the management, real-time analysis and monitoring, business policy enforcement, and other critical network intelligence for Videoscape Distribution Suite Internet Streaming (VDS-IS) and other 3rd party Content Delivery Networks (CDNs).

Document Conventions

This document uses the following conventions:

Table 1: Document Conventions

Convention	Description
^ or Ctrl	Both symbols represent the Control (Ctrl) key on the keyboard. For example, the key combinations **^D** or **Ctrl-D** means that you hold down the Control key while you press **D** . (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands, keywords, and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you need to enter values appear in *italic* font.
`Courier font`	Terminal sessions and information, which the system displays appear in `courier` font.

Convention	Description
Bold Courier font	Bold Courier font indicates the text that you must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive non-bolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material, which is not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader needs to be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning Means *reader beware.* In this situation, you might perform an action that could result in bodily injury.

Document Organization

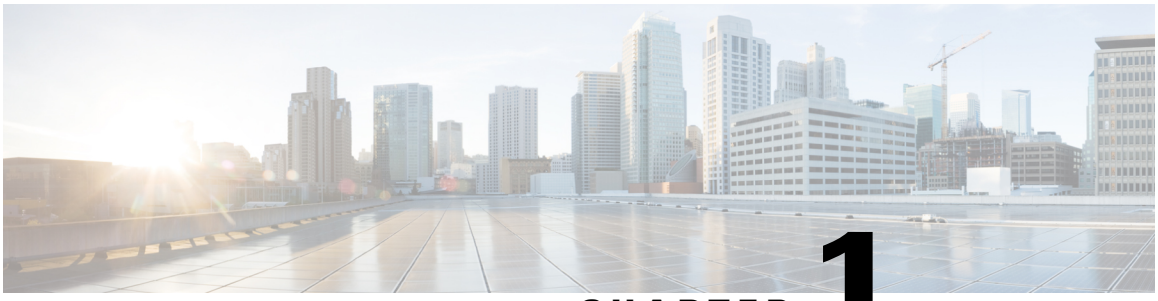
This document is organized into the following chapters:

Table 2: Document Organization

Chapter	Description
Getting Started	Provides information on getting started with VDS-SM 3.0.
Introduction to VDS-SM Portal's User Interface	Describes the VDS-SM user interface and general framework.
Home	Displays various scorecards such as network, protocol, content, and viewers.
Analytics	Displays various dashboards such as Analyze Metrics with Pivoting, Trends, and Reports.
Monitor	Displays various dashboards such as Throughput, Cache Hit Ratio, and Responses, which helps the CDN Operators to check the performance of the network
Alerts	Displays Manage Alerts menu, which lists a count of events that are generated by the system.
Configuration	Displays various dashboards such as Reseller and Content Provider.
Administration	Provides information on how to manage users and roles, an overview of the global configuration parameters, and how to configure SNMP.

Reporting Problems

If you have any query or experience problems when installing the VDS Service Manager software, contact your Cisco Technical representative.



CHAPTER 1

Getting Started

Getting Started

The VDS-SM provides configuration, management, real-time analytics and monitoring, business policy enforcement, and other critical network intelligence for VDS-IS. The solution installs on a VM infrastructure and operates on a customer's traditional computing system or a Cisco UCS system. This allows more efficient and focused use of computing resources, memory, and disk space; thus resulting in a more efficient ratio of computing resources to application performance.

Before you begin, ensure that the following tasks are completed as part of installation:

- Run configure indexers script (for details, see the section Adding an Analytics Indexer to VDS-SM in the Software Installation Guide)
- Schedule getCDStopology script in cron (for details, see the section Deploying CDS System Delivery Server/Services in Analytics Node in the Software Installation Guide)
- Install license

To install the Splunk license, perform the following steps:

1. Copy the Splunk license file to your local machine, taking care to note the location, which will be used later in this procedure.
2. Open the Splunk manager app in the Job Scheduler.

   Example, http://<IP of Job Scheduler>:8000/en-us/manager (**Username**: Admin or admin **Password:** Beaumaris1).

Note Do not change the above mentioned Splunk credentials. In the Change Password dialog, click **Skip** and proceed.

3 Select Licensing.

4 Select Add License.

5 Browse your machine to the location where you copied the license file.

6 Select Install.

7 Return to the Licensing page and confirm whether the new license is added and is valid.

Note Do not change the Splunk license filename.

Configuring Videoscape Distribution Suite Service Manager

VDS-SM discovers topology of Content Delivery Network (Service Engine, Service Router, and Distribution Hierarchy) and Delivery Services through CDSM. To initiate the discovery, you need to register the CDSM IP address along with the user credentials that is required to connect to CDSM.

Step 1 Login to VDS-SM using the link http://*UInode IP*/bnimgmt
Username: bniadmin and **Password**: admin

Step 2 From the main page, click **Configuration** > **CDN**.
To add CDN, see Adding a Content Delivery Network

Synchronization between VDS-SM and CDSM occurs at an interval of five minutes. After synchronization, the status will be displayed as 'Synchronization Successful'.

After synchronization, you can select the CDN and verify whether the devices and services information have been discovered.

Note Only Distribution Hierarchy and Delivery Services can be added or modified in VDS-SM.

Configuring CSV Files

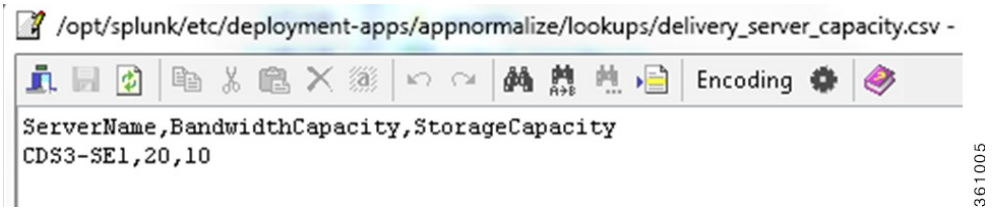
VDS-SM uses CSV files to map certain attributes with the log events. These CSV files need to be configured optionally for filters and for certain dashlets to be reflected in the user interface. The CSV files are located in the Job Scheduler node at the following location (**Username**: bnisplunk and **Password**: password):

/opt/splunk/etc/deployment-apps/appnormalize/lookups

Delivery_service_capacity.csv

This CSV file is used to enter the Bandwidth Capacity and Storage Capacity values for the Delivery Server that is being used.

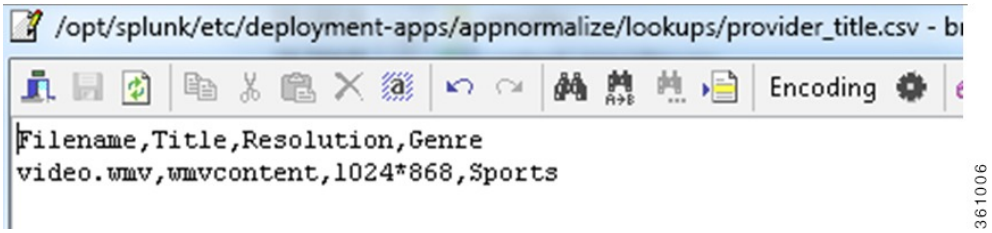
These values will be reflected in Throughput and Storage Capacity dashlets (these charts are available in Network scorecard and Trends).



Provider_title.csv

This CSV file is used to map the Filename of the content played with its Title, Resolution, and Genre.

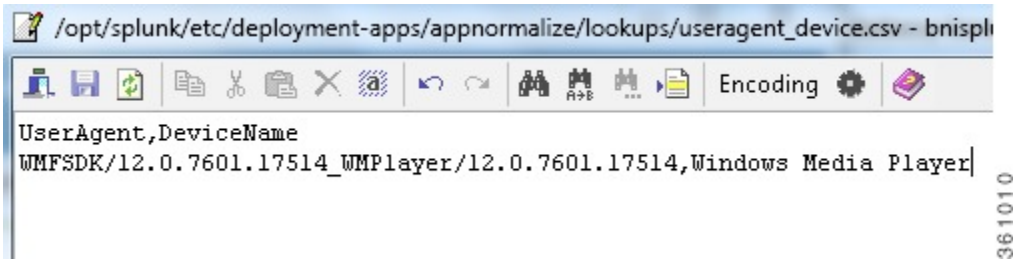
These values will be mapped under the respective filters in the Content scorecard.



User_agent.csv

This CSV file is used to map the user agent by which the content is played to its meaningful name (user defined).

These values will be reflected in the Top Content by Client Type dashlet (this chart is available in Viewers scorecard and Trends). However, if this CSV is not updated manually, the dashlet will be displayed by fetching the actual user agent of the client.



Configuring VDS-IS for VDS-SM

VDS-SM uses transaction logs that are generated by Service Router (SR) and Service Engine (SE) for analysis. Therefore, you need to configure SR and SE to enable logging and export them to VDS-SM.

Note There is a footer count mismatch issue in older versions of CDS-IS. As a result, the client session index will not be created. This will hinder certain dashlets from being populated in VDS-SM. Therefore, it is recommended that you use the following versions of CDS-IS:

- CDS-IS 3.2.0(B33)
- CDS-IS 3.2.1(B11)

Enable Transaction Log

To enable and export transaction logs, perform the following steps:

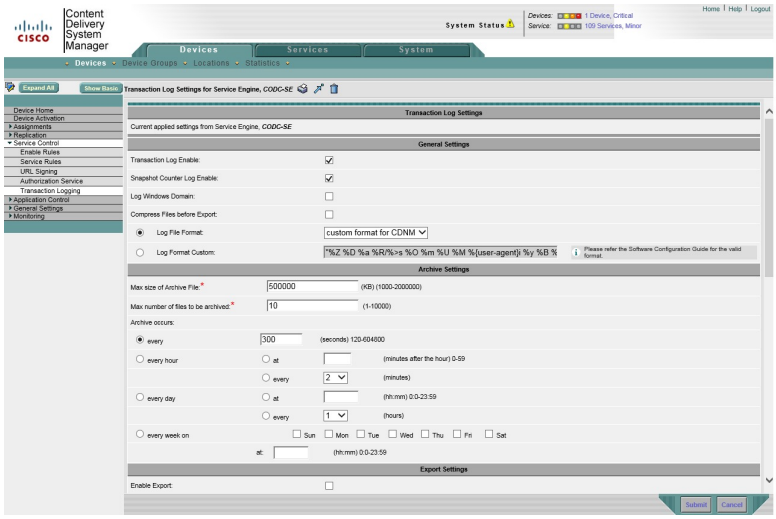
Step 1 Login to the CDSM UI.

Step 2 Click **Devices** and select the required SE.

Step 3 In the right pane, click **Service Control** > **Transaction Logging**.

Step 4 Check the **Transaction Log Enable** check box.

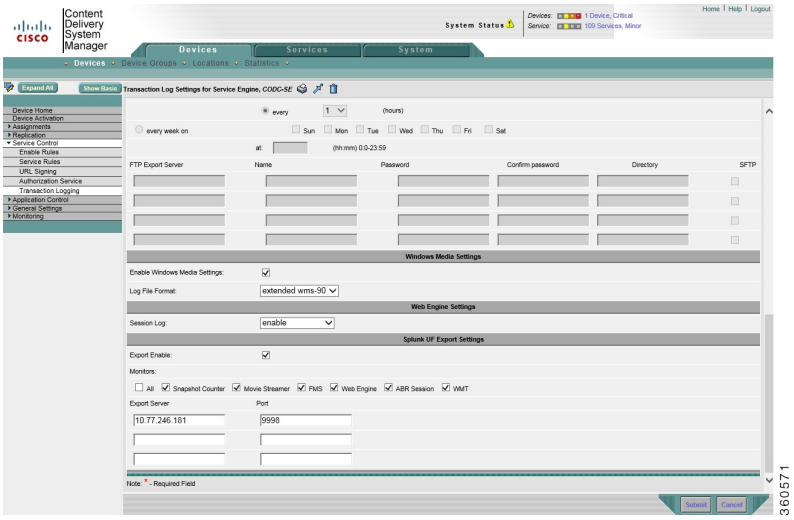
Step 5 From the **Log File Format** drop-down list, select **custom format for CDNM** option.



Step 6 From within **Archive Settings**, click **every** radio button and set the archive to 5 minutes (300 seconds).

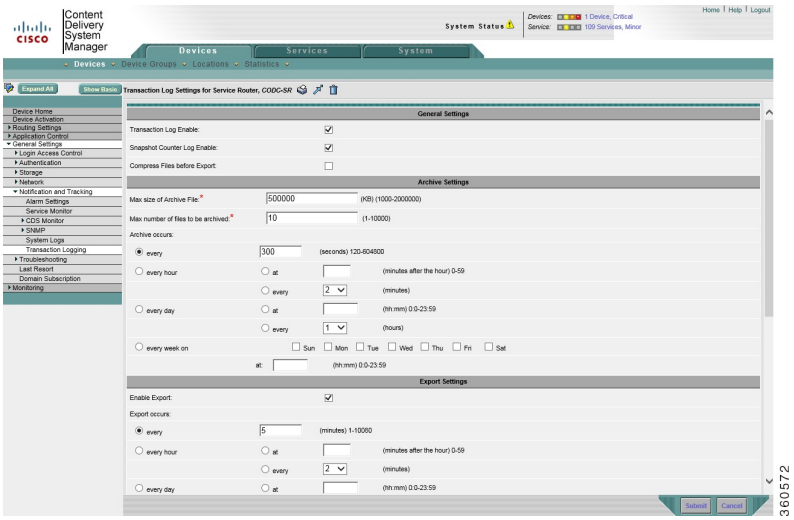
Note VDS-SM recommends that the archival time be set to 5 minutes. Exceeding this time interval would result in missing events (logs), which might hinder the dashboards from being populated.

Step 7 From within **Splunk UF Export Settings** (scroll down using the scroll bar), check the **Export Enable** check box, and check the type of logs that has to be logged (Snapshot Counter, FMS, Web Engine, ABR Session, WMT).



Step 8 Enter the VDS-SM Forwarder IP in the **Export Server** field and click **Submit**.
The following steps are necessary to populate the network scorecards and other SR related dashlets in VDS-SM.

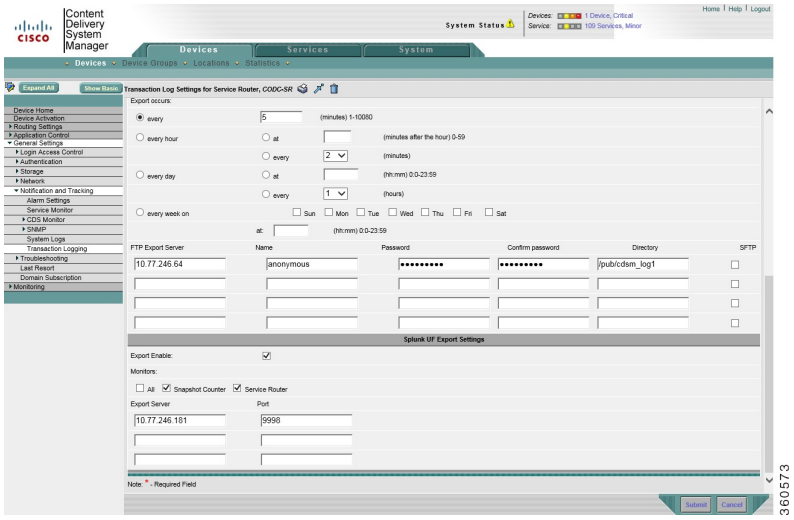
Step 9 Select **Devices** and select the required SR.



Step 10 In the right pane, click **General Settings** > **Notification and Tracking** > **Transaction Logging**.

Step 11 From within **Archive Settings**, click **every** radio button and set the archive to 5 minutes (300 seconds).

Step 12 From within **Splunk UF Export Settings** (scroll down using the scroll bar), check the **Export Enable** check box, and check the type of logs that has to be logged (Snapshot Counter and Service Router).



Enable Session Tracking for ABR Services

VDS-SM uses ABR session logs to analyze ABR sessions. Although the ABR session log is enabled as part of the previous step, the log will be generated only if session tracking is configured for the delivery services.

You can configure session tracking using CDSM as mentioned below:

1. Click **Services** and select the required delivery service.
2. In the left pane, select **Location settings** and enable the required protocol (HSS and HLS based tracking).

For more information, refer page 248 in the CDS-IS User Guide (http://www.cisco.com/en/US/docs/video/cds/cda/is/3_0/configuration_guide/is_cds_3_0_config.pdf)

CAVEAT: With VDS-IS 3.2, session tracking is supported only by SE at the edges. If SE from inner tiers are used to deliver content, then session tracking cannot be enabled on those SEs and the sessions will not be visible to VDS-SM.

Valid Rule File

A valid rule file must be present in CDSM to analyze the ABR protocols and bitrate fields. Select **System** > **Configuration** > **Authorization File Registration** (in the right pane).

Example

Following are rule file entries with fields for analyzing the ABR protocols.

<Rule_Allow matchGroup="grp1" protocol="http"/>

<Rule_SetAction name="Rule_DSConfig" matchGroup="grp1" protocol="http">

<SetParameter name="SessionResolveRule#1" value="(.*)**m3u8**(.*):none"/> *//m3u8 is the extension of the video played*

<SetParameter name="GenericSessionPlay#1" value="(.*)**ts**(.*):none"/>

<SetParameter name="SessionProtocol#1" value="(.*):protocol=$**generic_hls**"/> *//to map abr-protocol field from the log*

<SetParameter name="SessionBitrate#1" value="(.*)sample/(.*)/(.*):**bitrate**=$2"/> *//to map the bit rate fieldfrom the field*

<SetParameter name="SessionProfile#1" value="(.*)sample/(.*)/(.*):profile=$2"/>

Following are sample log file entries that are mapped using the above rule file entries.

#Software: (CDS 3.2.0 b8)

client-ip abr-protocol session-id manifest-uri asset-id bytes-sent bytes-recvd status time-recvd time-to-serve bitrate encryption session-tracking-mode status-code user-agent entry-gen-time mime-type profile

10.140.8.240 *generic_hls* 10f-I-617F44E4B4027469A848025065C227409629

http://hls.abr.com/sample/*sample.m3u8 - 514515 1663* bitrate_shift [10/Jan/2013:05:52:53.710+0000]

Note Make sure that proper quotas (Storage, Bandwidth, Session) are being allotted to Delivery Services in CDSM.

Verify Log Ingestion in VDS-SM

After enabling the export of log data using Splunk UF, SE and SR will connect to the VDS-SM Forwarder node and start ingesting data. You can verify the data flow in the system as mention in the Verify Connectivity Between VDS-IS and VDS-SM, on page 7 section.

Verify Connectivity Between VDS-IS and VDS-SM

You need to check whether the connection has been established or not between SE, SR, and the Forwarder node.

Step 1 SSH to VDS-SM Forwarder node.
Username: bnisplunk and **Password**: password

Step 2 Enter the command *netstat -na | grep 9998*

```
[bnisplunk@fwd local]$ netstat -na | grep 9998
tcp        0      0 0.0.0.0:9998                0.0.0.0:*                   LISTEN
tcp        0      0 10.77.240.180:9998          10.77.240.172:22697         ESTABLISHED
tcp        0      0 10.77.240.180:9998          10.77.240.172:37571         ESTABLISHED
tcp        0      0 10.77.240.180:9998          10.77.240.187:51503         ESTABLISHED
tcp        0      0 10.77.240.180:9998          10.77.240.187:54533         ESTABLISHED
tcp        0      0 10.77.240.180:9998          10.77.240.173:58895         ESTABLISHED
tcp        0      0 10.77.240.180:9998          10.77.240.173:26491         ESTABLISHED
[bnisplunk@fwd local]$
```

360574

Connection must be established between SE, SR, and the Forwarder node.

If the connection is not established, verify the connectivity between VDS-SM Forwarder node and the nodes in CDN.

Checking for Data in VDS-SM

VDS-SM aggregates data at different intervals to compute metrics. Therefore, expect some delay for the data to reflect in the dashboards.

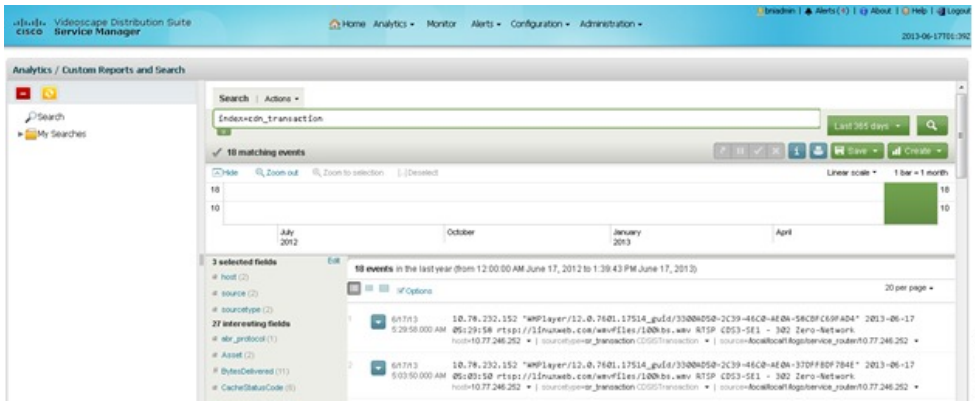
Note All the above steps need to be performed as a prerequisite before ingesting logs into VDS-SM.

The following table lists the different dashboards and the time they require to display the data:

Dashboard	Time Required
Monitor	Less than 15 minutes
Network Scorecard	1 Hour
Protocol Scorecard	1 Hour
Content Scorecard	1 Day
Viewers Scorecard	1 Day
Trends	1 Day
Content and Session Analytics	1 Day

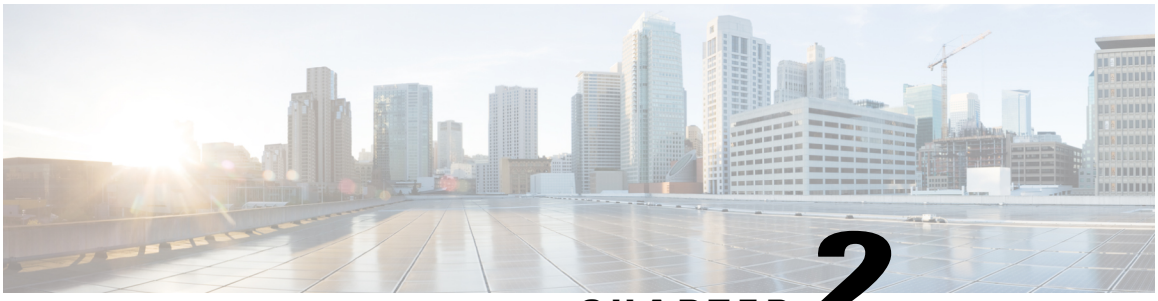
Step 1 Login to VDS-SM using the link http://UInode IP/bnimgmt
Username: bniadmin and **Password**: admin

Step 2 Click **Analytics** > **Custom Searches and Reports**.
In the Search page, query for the respective index and check whether the data is indexed. After playing various video formats, the corresponding dashboards will be populated in VDS-SM.



Monitor dashboard can be used to check the data flow into VDS-SM at real-time (with minimal delay).

Dashboard	Remarks
Network scorecard > 24 hours (default time)	Displays data for the last 24 hours.
Network Scorecard > 60 minutes	Displays data for the last 60 minutes (current time minus 10 minutes).
Network Scorecard > 7 days	Displays data for the last 7 days.
Protocol Scorecard > 60 minutes (default)	Displays data for the last 60 minutes (current time minus 10 minutes).
Protocol Scorecard > 24 hours	Displays data for the last 24 hours.
Protocol Scorecard > 7 days	Displays data for the last 7 days.
Content Scorecard > Previous day (default)	Displays the previous day's data.
Content Scorecard >7 days	Displays data for the last 7 days.
Viewers Scorecard > Previous day (default)	Displays the previous day's data.
Viewers Scorecard >7 days	Displays data for the last 7 days.
Monitor	Displays data for every 5 minutes with 1 minute delay.
Trends	Displays data for last 7 days by default.



CHAPTER 2

Introduction to Videoscape Distribution Suite Service Manager Portal's User Interface

Videoscape Distribution Suite Service Manager Overview

The VDS-SM provides configuration, management, real-time analytics and monitoring, business policy enforcement, and other critical network intelligence for VDS-IS. CDN hosts different content, such as live and archived, to viewers around the world. It helps the CDN Operators to quickly check the performance of the network.

The VDS Manager software includes the following major components:

- Analytics—Creates a fast searchable index of CDN streaming device log files for centralized access.
- Provisioning—Provides the Administration team the rights to create new Delivery Services and to control CDN from the same interface, which is used for analytics retrieval.
- Reporting—Provides a single interface for provisioning and reporting CDN solutions that may reside in a single provider's environment (for example, VDS-IS).

The application nodes that comprise the VDS-SM solution are Java applications deployed within a JBOSS application server, and is separated into distinct "solutions", each of which provides a specific set of services for the overall application.

VDS-SM Application Nodes

The VDS-SM supports the following application nodes:

- Core Services
- User Interface

- CDN Manager
- Analytics

Core Services

The Core Services node includes the following:

- Management Interface—This interface provides service registry, SNMP support, and stores global configuration parameters, for the management of solution nodes.
- Database—Hosts the MySQL database that is used to store the configuration information including topology, solution tables, and registry information.

User Interface

Presents a User Interface where status, configuration, and analytics can be viewed by the Operator.

CDN Manager

Provides management services for CDN including Cisco VDS-IS.

Analytics

Analytics includes the following nodes:

- Search Head—Provides search and reporting functions.
- Forwarder—Manages the distribution of log data from CDN to Analytics Infrastructure for processing.
- Indexer—Processes log data to facilitate fast data retrieval and reporting.
- Job Scheduler—Provides job scheduling and functions as a deployment repository for the analytics software.

Logging Into the User Interface

Enter your Username and Password in the Login window.

By default, the username is **bniadmin** and the password is **admin**. If required, you can change the username and password after initial log in.

To log out of the user interface, click **Logout**, located on the top-right corner of the window.

Changing Your Password

To change your password, click the <*User Profile*> button, for example, **bniadmin**, located in the menu bar, to open the User Info dialog.

User Info Dialog

To increase security, we recommend that you use a combination of letters, numbers and characters.

VDS-SM Portal's User Interface Overview

This section provides an overview of the VDS-SM Portal's user interface.

Note Before you access the VDS-SM Portal's user interface, you must deploy, install, and configure, all nodes in your network.

VDS-SM comprises the following functions:

Table 3: VDS-SM Functionalities & Description

Function	Description
Home	Displays the following scorecards: • Network • Protocol • Content • Viewers

Function	Description
Analytics	Displays the following menus and submenus: • Analyze Metrics with Pivoting • Trends • Reports • Customs Searches and Reports • Custom Dashboards • Content–Analyze by Content Title and Viewership Report • Sessions–Analyze by Content IP
Monitor	Helps the CDN Operators check the performance of the network.
Alerts	Displays Manage Alerts menu.
Configuration	Displays the following menus and submenus: • CDN • Customers–Reseller and Content Provider • Services
Administration	Displays the following menus: • System Load Dashboard • User Management • SNMP Trap Destinations • Global Configurations

User Interface Components

The user interface components are explained in the following table:

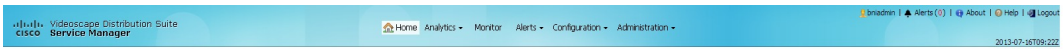
Table 4: User Interface Components

Component	Description
User Profile	To change your password, click the <*User Profile* > button; for example, **bniadmin**, located in the top-right corner of the window, to open the User Info dialog box. **Note** The button name displays the name of the user logged in.
Alert Counter	Lists the alert notifications. Click **Alerts**, located next to User Profile. It displays the alerts you set up.
About Dialog	Click **About**, located next to Alert, to display the About dialog box. The following information about the VDS-SM Portal's software is mentioned: • Product Version • Product Name • Build Timestamp • Build Number • Build Java Version • Software Licenses • End User Licenses Agreement
Logout	Click **Logout**, located next to Help, to log out from the application.
Home	Displays the following scorecards: • Network • Protocol • Content • Viewers

Component	Description
Analytics	Displays the following menus and submenus: • Analyze Metrics with Pivoting • Trends • Reports • Customs Searches and Reports • Custom Dashboards • Content–Analyze by Content Title and Viewership Report • Sessions–Analyze by Content IP
Monitor	Displays the following dashlets: • Services • Network • Throughput • Cache Hit Ratio • Concurrent Active Sessions • Responses
Alerts	Displays the Manage Alerts menu.
Configuration	Displays the following menus and submenus: • CDN • Customers–Reseller and Content Provider • Services
Administration	Displays the following menus: • System Load Dashboard • User Management • SNMP Trap Destinations • Global Configurations

Main Menu

The main menu bar displays all VDS-SM tabs. Click the menus to view the submenus.

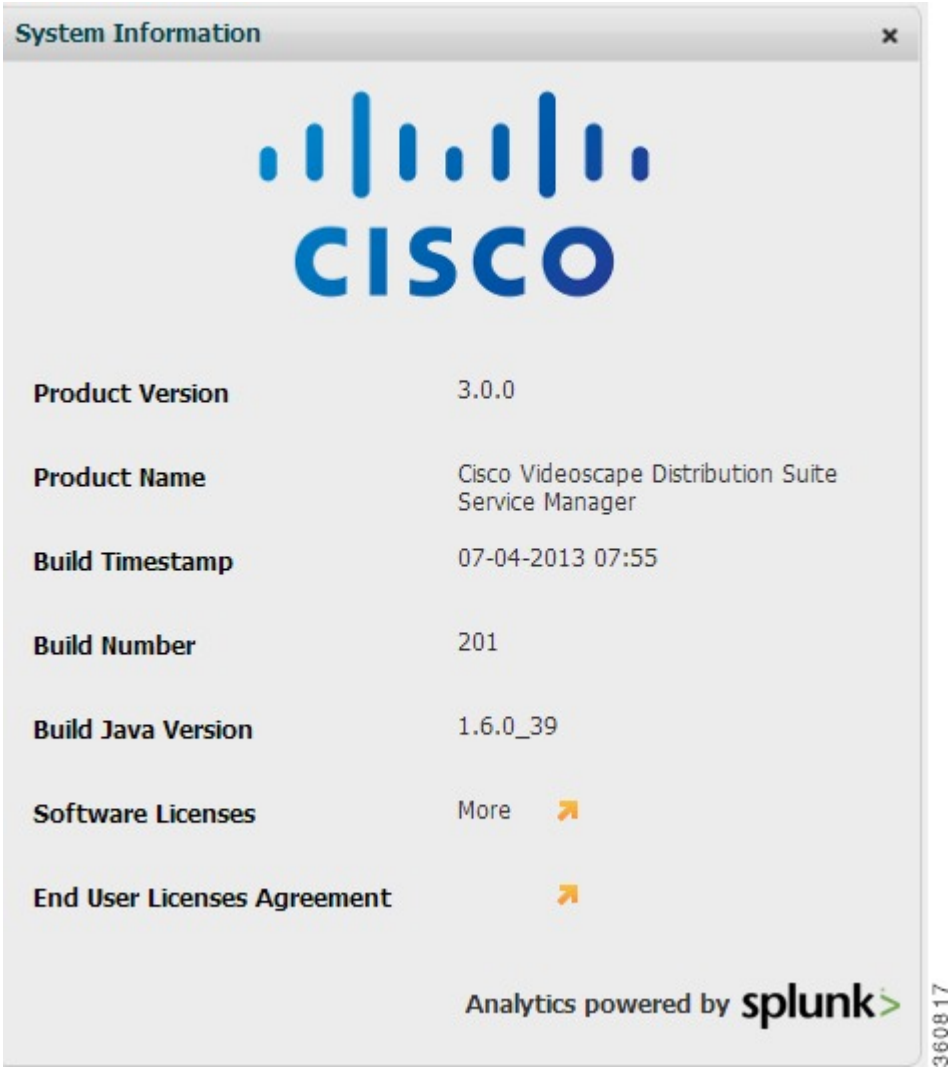


About Dialog

The VDS-SM Portal's **About** dialog lists the following information:

- Product Version Number
- Product Name
- Build Timestamp
- Build Number
- Build Java Version
- Software Licenses
- End User Licenses Agreement

To access this dialog, click **About** at the top of the page.



Note Click the orange arrow next to the item to see more information.

Configuration Icons

VDS-SM portal provides various icons to perform configuration commands or to indicate operational status. The following table lists all the icons included in the user interface.

Table 5: User Interface Icons

Icon	Description
	Go to Detail page

Icon	Description
	Create or Add
	Delete
	Undo
	Refresh
	Disable
	Enable
	Clone
	Import
	Edit: in-line mode: • Select: light gray
	Edit: full-screen mode: • Select: light gray
	Edit: bulk mode: • Select: light gray • Deselect: dark gray
	Edit: Item Selector
	Information
	Auto Refresh
	Context Sensitive Help
	Search; Filter

Icon	Description
	Notice
	Normal
	Added
	Deleted
	Edited
	View
	Export
	Add Volumes
	Remove Volumes
	Operational State: Up
	Operational State: Down
	Synchronization

Role Based Access Control

Role Based Access Control (RBAC) is implemented in VDS-SM. Delivery Services and Providers drop-down lists are filtered, based on the user logged into the system.

The following figure shows the permissions granted for CDN Operator Admin, CDN Operator Viewer, Reseller Admin, Reseller Viewer, Content Provider Admin, and Content Provider Viewer.

Main Menu	Navigation	CDNOpr Admin				CDNOpr Viewer				Reseller Admin				Reseller Viewer				CP Admin				CP Viewer			
		Accessible?	Permission?		Test Passed?	Accessible?	Permission?		Test Passed?	Accessible?	Permission?		Test Passed?	Accessible?	Permission?		Test Passed?	Accessible?	Permission?		Test Passed?	Accessible?	Has Permission?		Test Passed?
			View	Edit			View	Edit			View	Edit			View	Edit			View	Edit			View	Edit	
Home	Scorecards	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓
Analytics	Analyze Metrics with Pivoting	✓	✓	NA	✓	✓	✓	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Analytics	Trends	✓	✓	NA	✓	✓	✓	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Analytics	Reports	✓	✓	NA	✓	✓	✓	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Analytics	Custom Search and Reports	✓	✓	✓	✓	✓	✓	✓	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Analytics	Custom Dashboards & Reports	✓	✓	✓	✓	✓	✓	✓	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Analytics	Content-> Analyze by Content Title	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓
Analytics	Content-> Viewership Report	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓
Analytics	Sessions-> Analyze by Client IP	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓
Configuration	CDN	✓	✓	✓	✓	✓	✓	×	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Configuration	Customers -> Reseller	✓	✓	✓	✓	✓	✓	×	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Configuration	Customers -> Reseller Profile	×	NA	NA	✓	×	NA	NA	✓	✓	✓	✓	✓	✓	✓	×	✓	×	NA	NA	✓	×	NA	NA	✓
Configuration	Customers -> Content Provider	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	×	✓	×	NA	NA	✓	×	NA	NA	✓
Configuration	Customers -> Content Provider Profile	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	✓	✓	✓	✓	✓	✓	✓	✓
Configuration	Customers -> Services	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓	✓	✓	NA	✓
Administration	System Load Dashboard	✓	✓	✓	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Administration	User Management	✓	✓	✓	✓	×	NA	NA	✓	✓	✓	✓	✓	×	NA	NA	✓	✓	✓	✓	✓	×	NA	NA	✓
Administration	SNMP Trap Destinations	✓	✓	✓	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Administration	Global Configurations	✓	✓	✓	✓	✓	✓	×	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Monitor	Monitor	✓	✓	✓	✓	✓	✓	✓	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Alerts	Alerts -> Thresholds	✓	✓	✓	✓	✓	✓	✓	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓
Alerts	Alerts -> Manager Alerts	✓	✓	✓	✓	✓	✓	✓	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓	×	NA	NA	✓

361594

Access privileges are determined by the role assigned to the user. A user may be granted privileges for all or some system configuration and management functions.

The following table lists the access privilege to Reseller Admin.

Main Menu and Navigation	Reseller Admin
Home > Scorecards	• Delivery Service and Provider drop-down lists will be filtered for the Reseller. • View results and Analyze data link will not be available.
Analytics > Content > Analyze by Content Title	Delivery Service and Provider drop-down lists will be filtered for the Reseller.
Analytics > Content > Viewership Report	Delivery Service and Provider drop-down lists will be filtered for the Reseller.
Analytics > Sessions > Analyze by Client IP	Delivery Service and Provider drop-down lists will be filtered for the Reseller.
Configuration > Customers > Services	Data will be filtered for the Reseller.

The following table lists the access privilege to Reseller Viewer.

Main Menu and Navigation	Reseller Viewer
Home > Scorecards	• Delivery Service and Provider drop-down lists will be filtered for the Reseller. • View results and Analyze data link will not be available.
Analytics > Content > Analyze by Content Title	Delivery Service and Provider drop-down lists will be filtered for the Reseller.

Main Menu and Navigation	Reseller Viewer
Analytics > Content > Viewership Report	Delivery Service and Provider drop-down lists will be filtered for the Reseller.
Analytics > Sessions > Analyze by Client IP	Delivery Service and Provider drop-down lists will be filtered for the Reseller.
Configuration > Customers > Services	Data will be filtered for the Reseller.

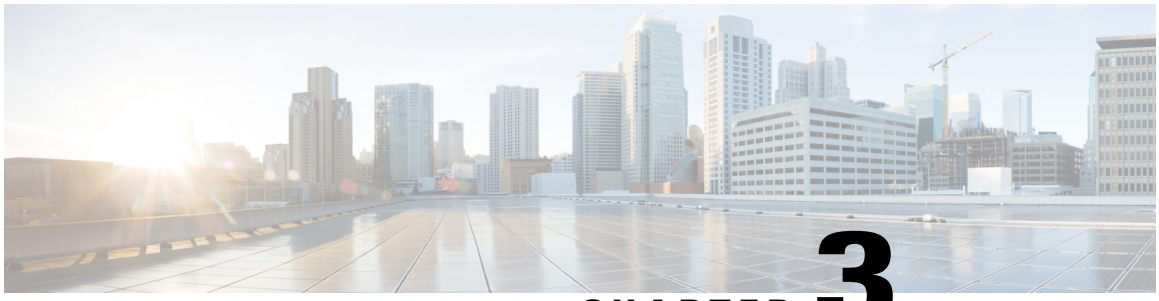
The following table lists the access privilege to Content Provider Admin.

Main Menu and Navigation	Content Provider Admin
Home > Scorecards	• Delivery Service and Provider drop-down lists will be filtered for the Content Provider. • View results and Analyze data link will not be available.
Analytics > Content > Analyze by Content Title	Delivery Service and Provider drop-down lists will be filtered for the Content Provider.
Analytics > Content > Viewership Report	Delivery Service and Provider drop-down lists will be filtered for the Content Provider.
Analytics > Sessions > Analyze by Client IP	Delivery Service and Provider drop-down lists will be filtered for the Content Provider.
Configuration > Customers > Services	Data will be filtered for the Content Provider.

The following table lists the access privilege to Content Provider Viewer.

Main Menu and Navigation	Content Provider Viewer
Home > Scorecards	• Delivery Service and Provider drop-down lists will be filtered for the Content Provider. • View results and Analyze data link will not be available.
Analytics > Content > Analyze by Content Title	Delivery Service drop-down list will be filtered for the Content Provider.
Analytics > Content > Viewership Report	Delivery Service and Provider drop-down lists will be filtered for the Content Provider.

Main Menu and Navigation	Content Provider Viewer
Analytics > Sessions > Analyze by Client IP	Delivery Service and Provider drop-down lists will be filtered for the Content Provider.
Configuration > Customers > Services	Data will be filtered for the Content Provider.



CHAPTER 3

Home

Home Overview

The logs from VDS-IS are summarized and indexed in VDS-SM. The enormous information present in logs are displayed in charts to help the operators understand their CDN network. This provides an holistic view of a CDN.

On logging into the application, the Home page is displayed. It includes various scorecards. A scorecard is a dashboard, which displays specific information about network, protocol, content, and viewers data of managed CDN.

Home tab includes the following scorecards:

- Network
- Protocol
- Content
- Viewers

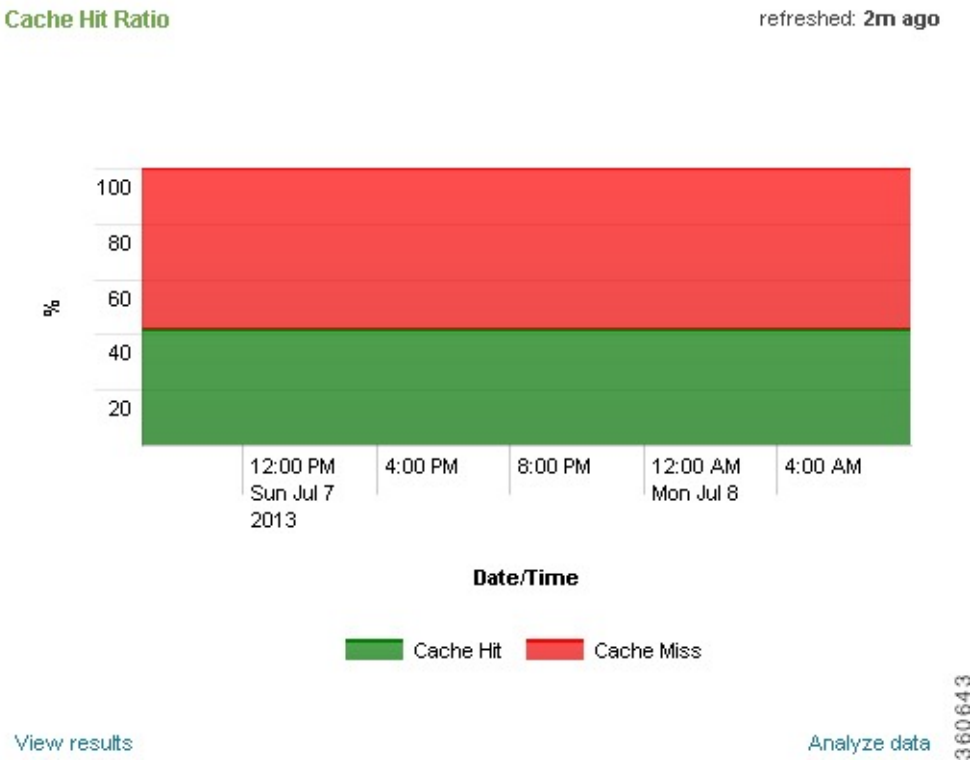
Using Scorecards

Using scorecards, you can:

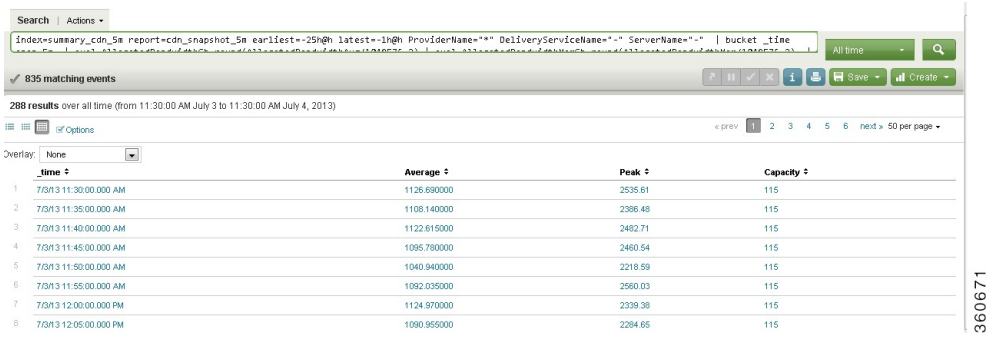
- Mouse hover a specific point within a chart, which displays additional information such as time and parameters.

- View results

  Each chart provides access to view the log information corresponding to the dashlets. Click **View results**, located at the bottom left of each chart, to view the report.



From within the source report, you can choose a desired row to display the log details for the item.



- Analyze data

  The chart in few scorecards contain data at a high-level. The CDN Operators have the option to drill down the data in the chart at a granular level. Click **Analyze data**, located at the bottom right of the chart, to view the details. Here, the CDN Operators can view the data plotted using various metrics over different dimensions that are split by the required dimension.

  You can also view the data represented in different charts, such as line, bar, area and pie, by clicking the **Chart type** drop-down list, which appears after you click **Analyze data**.

  Click **Analyze**, **of**, **over**, and **split by** drop-down lists and select the required options. You can also select the stack mode from the **Stack mode** drop-down list.

Legend

Depending on the chart, if more than one data set is displayed, a legend is located below the chart.

Lookups

Lookup is a process, which replaces the raw data from the logs with meaningful information. In VDS-SM, lookups are performed during summary index creation and chart rendition. CSV files and third party databases are used in the lookup operations.

Following is the list of lookups:

Lookup Name	Description
Title	The raw logs has the URL field, which contains the 'asset' information. Lookup is performed on provider_title.csv file to get a meaningful Title name. This lookup is performed during summarization.
Genre, Resolution	The raw logs do not contain any information on Genre and Resolution. Based on 'asset', the Genre and Resolution are looked up from provider_title.csv file. This lookup is performed during summarization.
Bitrate	The ABR traffic type's (HLS and MobiTV) raw logs have 'profile name' to indicate bitrate. Lookup is performed on profilename_bitrate.csv to get the related bitrates for profile names. This lookup is performed during summarization.
ISP, Net Sped	The raw logs do not contain information on ISP and Net Speed. It has ClientIP. Lookup is performed on Maxmind DB using ClientIP to get ISP and Net Speed. The Lookup works for public IP addresses. This lookup is performed during summarization.

Lookup Name	Description
City	The raw logs do not contain the City information. It has ClientIP. Lookup is performed on Maxmind DB using ClientIP to get City. The Lookup works for public IP addresses. This lookup is performed during chart rendition.
Client Type	The raw logs has User Agent related information. Lookup is performed on useragent_device.csv file using User Agent to get Client Type. This lookup is performed during summarization.
Capacity	The Bandwidth and Storage capacity of Delivery Servers are maintained in the delivery_server_capacity.csv file. These capacity values are looked up and added to the summary indexes during summarization.
Provider	When CP lookup is implemented, users extract CP ID from the URL. Lookup is performed on content_provider.csv file using CP ID to get CP name. This lookup is performed during summarization.

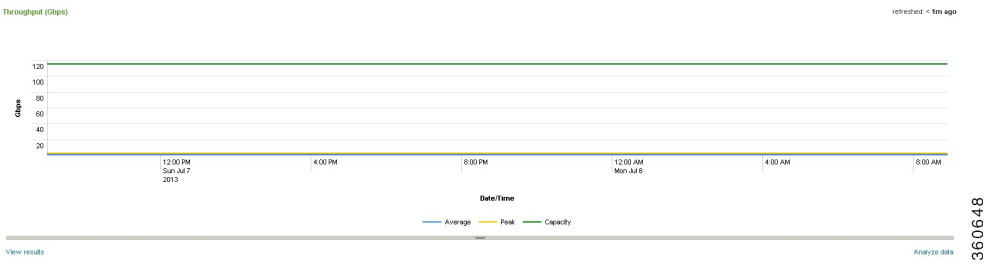
Network

When you launch the application, by default, the Network tab is displayed in the Home page. This scorecard displays charts that provides the users a quick overview on the overall performance of the network. By default, the data for the last 24 hours is displayed in the scorecard.

The following metrics are displayed here:

- Throughput (Gbps)
- Cache Hit Ratio by Location
- Cache Hit Ratio
- Origin/Ingest Volume
- Concurrent Active Sessions
- Response Status Codes
- Storage Usage

Throughput



The following table describes the chart within this scorecard:

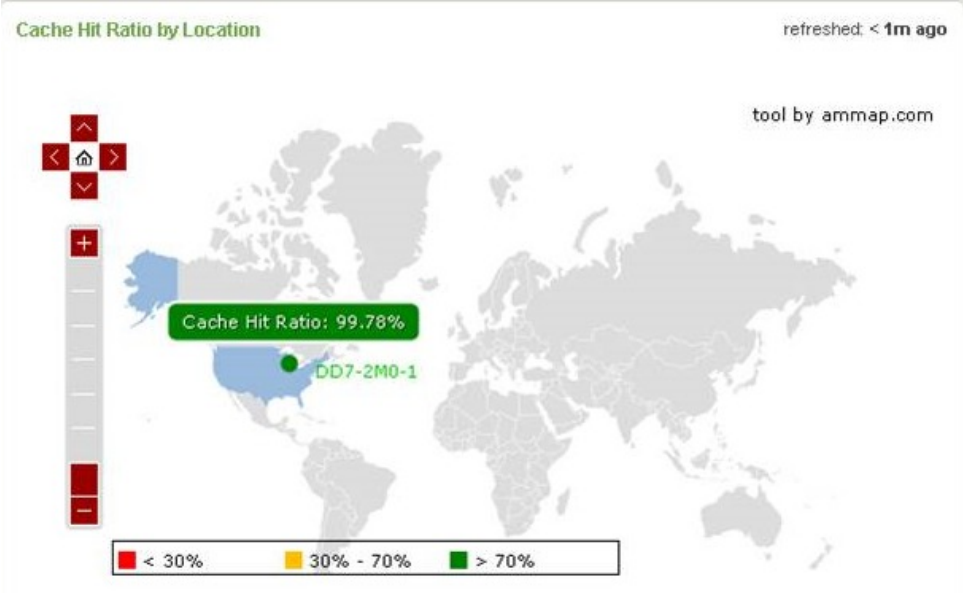
Table 6: Throughput Chart & Description

Chart	Description
Throughput (Gbps)	Illustrates the bandwidth delivered by the network, for the specified time interval.
Chart Information	The information within this chart is shown in a line graph with Date/Time along the X-axis and Peak Throughput, Average Throughput, and Capacity in Gbps along the Y-axis. The legends are Peak, Average, and Capacity.
Chart Formula	The formula used to derive the peak and average throughput graph is: the maximum and mean throughput for the specified time interval.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Note If requests are made directly to the service engine without the service router, this dashlet will not be displayed.

Cache Hit Ratio by Location

This map displays all the delivery servers serving content to the end users with respect to cache hit ratio. The country in which the server is present will be highlighted. Based on the Cache Hit Ratio value of each server, the point will be plotted in different colors as mentioned below.



- If the cache hit ratio is less than 30 percent, the point will appear in red.
- If the cache hit ratio is between 30 and 70 percent, the point will appear in amber.
- If the cache hit ratio is greater than 70 percent, the point will appear in green.

Note The public IPs that are not resolved by MaxMind will be represented as '-' in the maps.

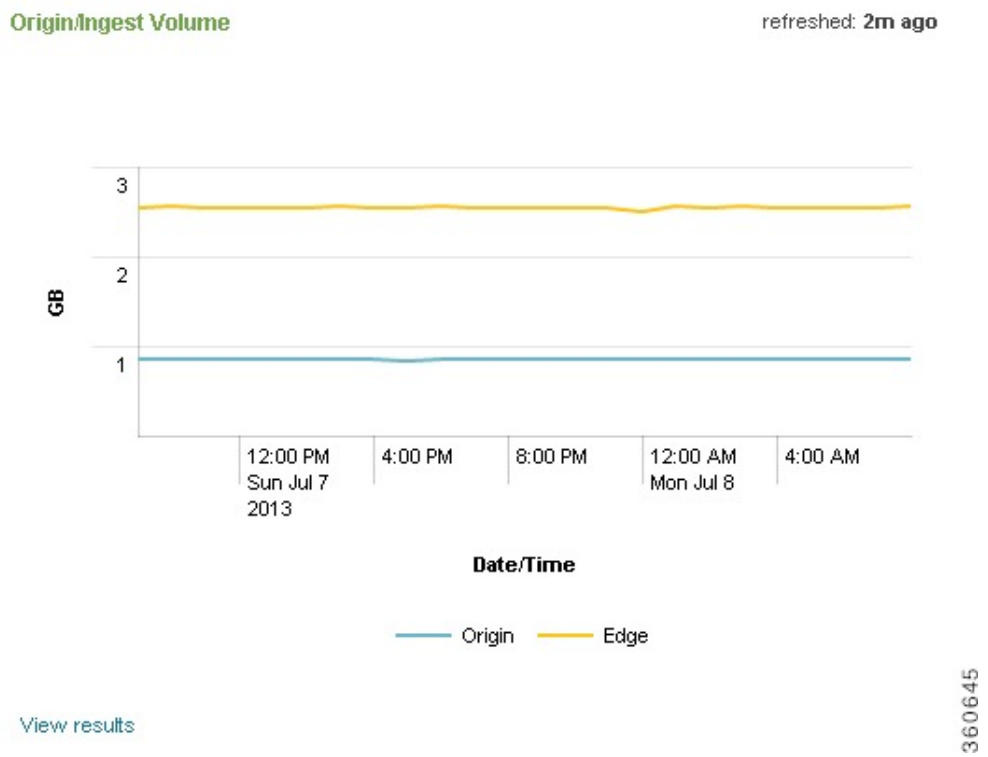
Cache Hit Ratio

The following table describes the chart within this scorecard:

Table 7: Cache Hit Ratio Chart & Description

Chart	Description
Cache Hit Ratio	Provides client request cache hit and miss percentage, for the specified time interval.
Chart Information	The information within this chart is shown in a stacked area graph with Date/Time along the X-axis and the cache hit and miss percentage in the Y-axis. The legends representing the graph are Cache Hit and Cache Miss.
Chart Formula	The formula used to derive the cache hit graph is: the percentage of cache hit over total requests. The formula used to derive the cache miss graph is: the percentage of cache miss over total requests.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Origin/Ingest Volume

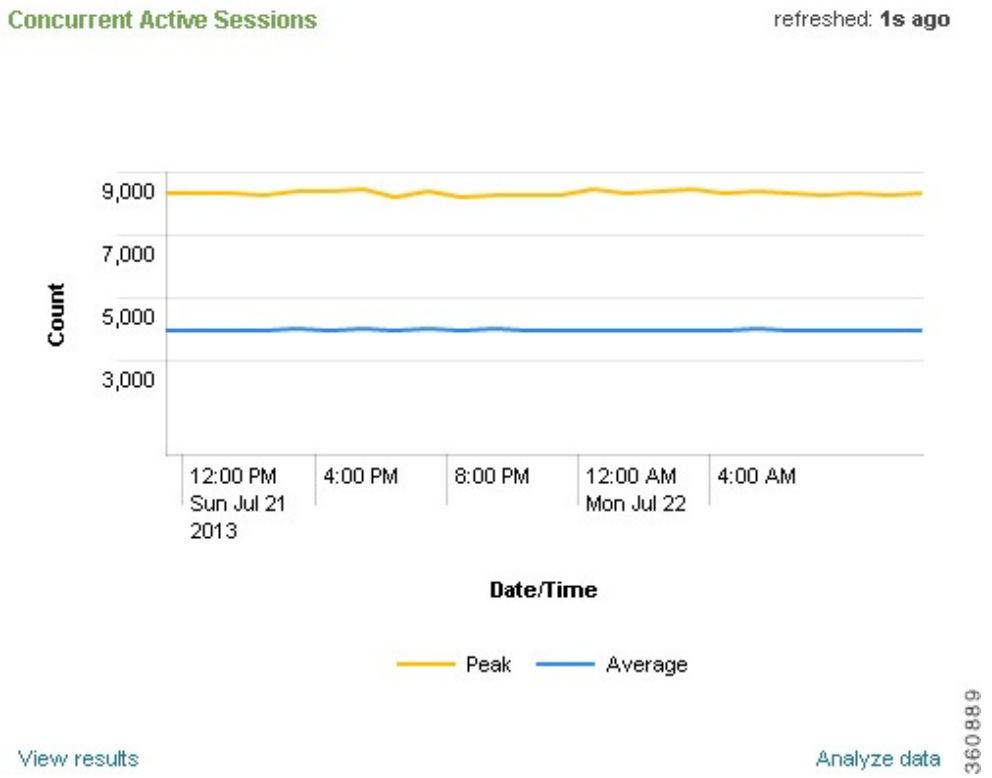


The following table describes the chart within this scorecard:

Table 8: Origin/Ingest Volume Chart & Description

Chart	Description
Origin/Ingest Volume	Illustrates the comparison between the prefetched content and dynamic content, for the specified time interval.
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and the Origin and Edge Volume in GB along the Y-axis.
Chart Formula	The formula used to derive the graph for Ingest is: sum of cache hit, cache miss, and no cache code. The formula used to derive graph for Origin is: cache miss bytes by Origin Server.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Concurrent Active Sessions



The following table describes the chart within this scorecard:

Table 9: Concurrent Active Sessions Chart & Description

Chart	Description
Concurrent Active Sessions	Illustrates the concurrent active sessions, for the specified time interval.
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and the Peak and Average Count along the Y-axis. The legends representing the graph are Peak and Average.
Chart Formula	The formula used to derive the graph is: calculate the maximum and mean active sessions, for the specified time interval.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Note If requests are made directly to service engine without service router, this dashlet will not be populated.

Response Status Codes

The following table describes the chart within this scorecard:

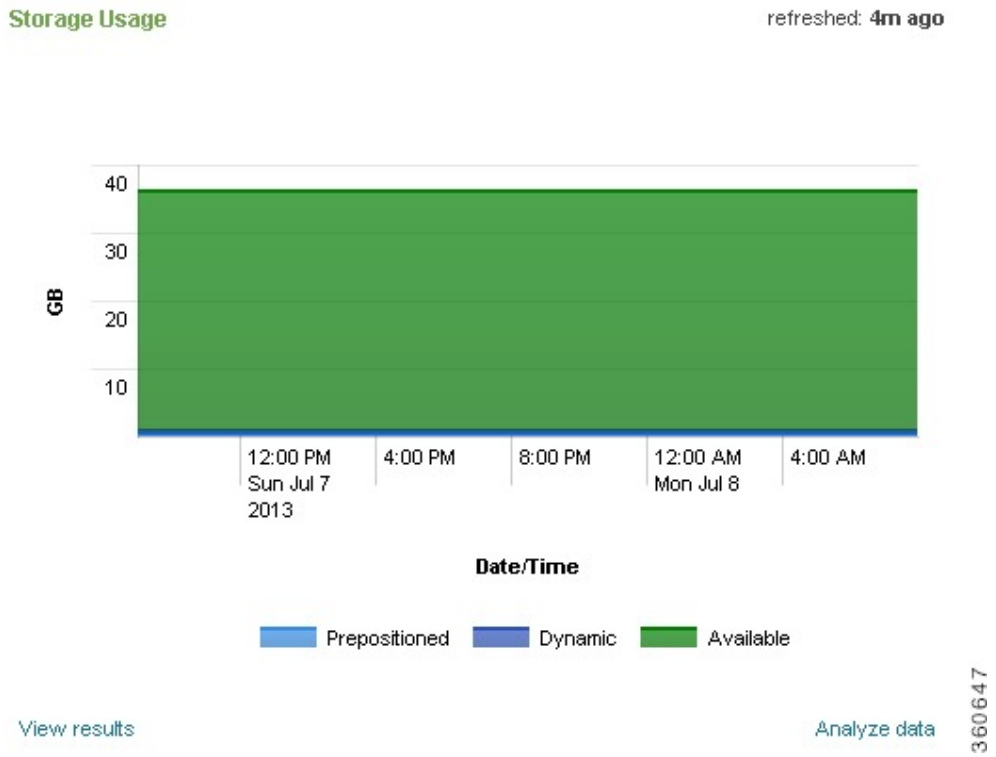
Table 10: Response Status Codes Chart & Description

Chart	Description
Response Status Codes	Provides response codes count and percentage, for the specified time interval.
Chart Information	The information within this chart is shown in stacked area with Date/Time along the X-axis with the response count and percentage along the Y-axis. The legends representing the graph are 2xx, 3xx, 4xx, and 5xx.
Chart Formula	The status code from logs are grouped as 2xx, 3xx, 4xx, and 5xx. The count of each group is calculated as the sum of individual status code counts. The percentage of each group is derived by calculating the percentage of group count over total responses.

Chart	Description
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

To view the response status code in percentage and count, click the respective radio buttons located above the chart.

Storage Usage



The following table describes the chart within this scorecard:

Table 11: Storage Usage Chart & Description

Chart	Description
Storage Usage	Illustrates the storage usage for the specified time interval.

Chart	Description
Chart Information	The information within this chart is shown in a stacked area graph with the Date/Time along the X-axis and the storage usage as Prepositioned, Dynamic, and Available in GB along the Y-axis. The legends representing the graph are Prepositioned, Dynamic, and Available.
Chart Formula	The prepositioned and dynamic values are derived by calculating the average of prepositioned and dynamic data, for the specified time interval. The available capacity is derived by calculating the difference between the storage capacity (as specified in the delivery_server_capacity.csv file) and the sum of prepositioned plus dynamic data.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Protocol

This tab displays charts that provides an overview of the network at the protocol level. By default, the data for the last 60 minutes is displayed in the scorecard.

To access this tab, click **Home** > **Protocol**.

The following metrics are displayed here:

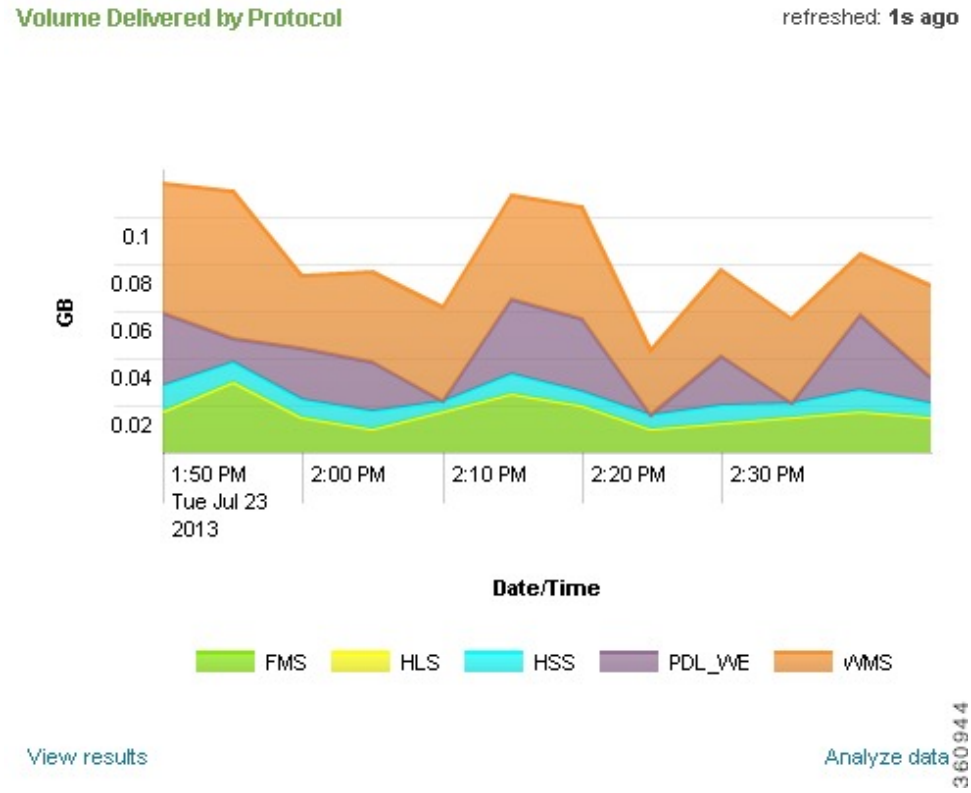
- Geographical Distribution of Protocols
- Volume Delivered by Protocol
- Total Requests by Protocol
- Response Codes by Protocol
- Cache Hit Ratio by Protocol
- ABR Session Bitrate by Protocol
- 4xx Errors by Protocol

Geographical Distribution of Protocols

This map displays all the delivery servers serving content to the end users with respect to protocols. The country in which the server is present will be highlighted. When you mouse hover a Delivery Server, the protocol that has served the maximum from that server and the corresponding bytes delivered will be displayed.

Note The public IPs that are not resolved by MaxMind will be represented as '-' in the maps.

Volume Delivered by Protocol

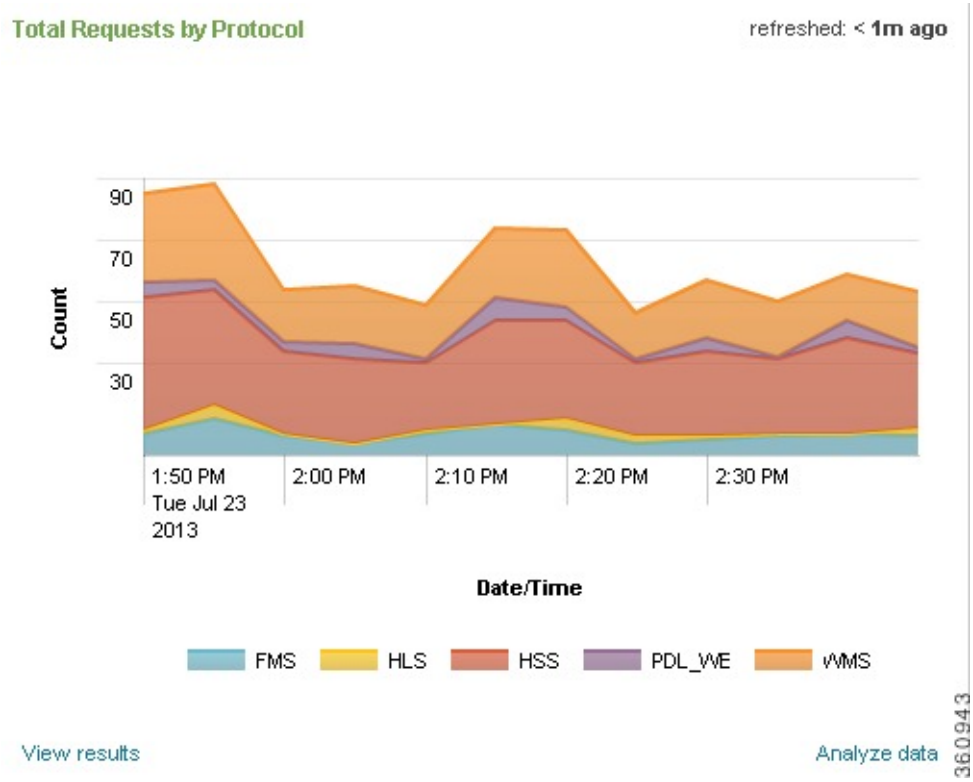


The following table describes the chart within this scorecard:

Table 12: Volume Delivered by Protocol Chart & Description

Chart	Description
Volume Delivered by Protocol	Illustrates the volume delivered by each protocol, for the specified time interval.
Chart Information	The information within this chart is shown in a stacked area graph with Date/Time along the X-axis and the volume delivered in GB along the Y-axis. The legends representing the graph are protocols.
Chart Formula	The formula used to derive the graph is: Total of CacheMissBytes, CacheHitBytes, and NoCacheCodeBytes grouped by Protocol.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Total Requests by Protocol

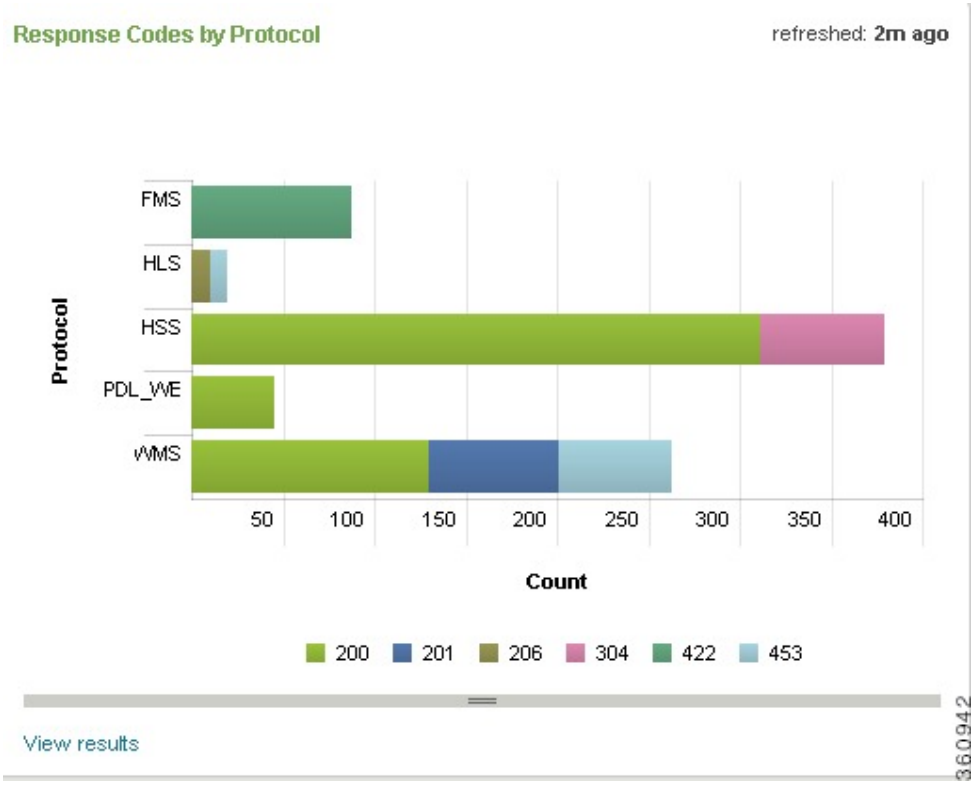


The following table describes the chart within this scorecard:

Table 13: Total Requests by Protocol Chart & Description

Chart	Description
Total Requests by Protocol	Illustrates the number of requests received from each protocol, for the specified time interval.
Chart Information	The information within this chart is shown in a stacked area graph with Date/Time along the X-axis and the request Count along the Y-axis. The legends representing the graph are protocols.
Chart Formula	The formula used to derive the graph is: Total Requests is the sum of all Status Code Counts grouped by Protocol.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Response Codes by Protocol

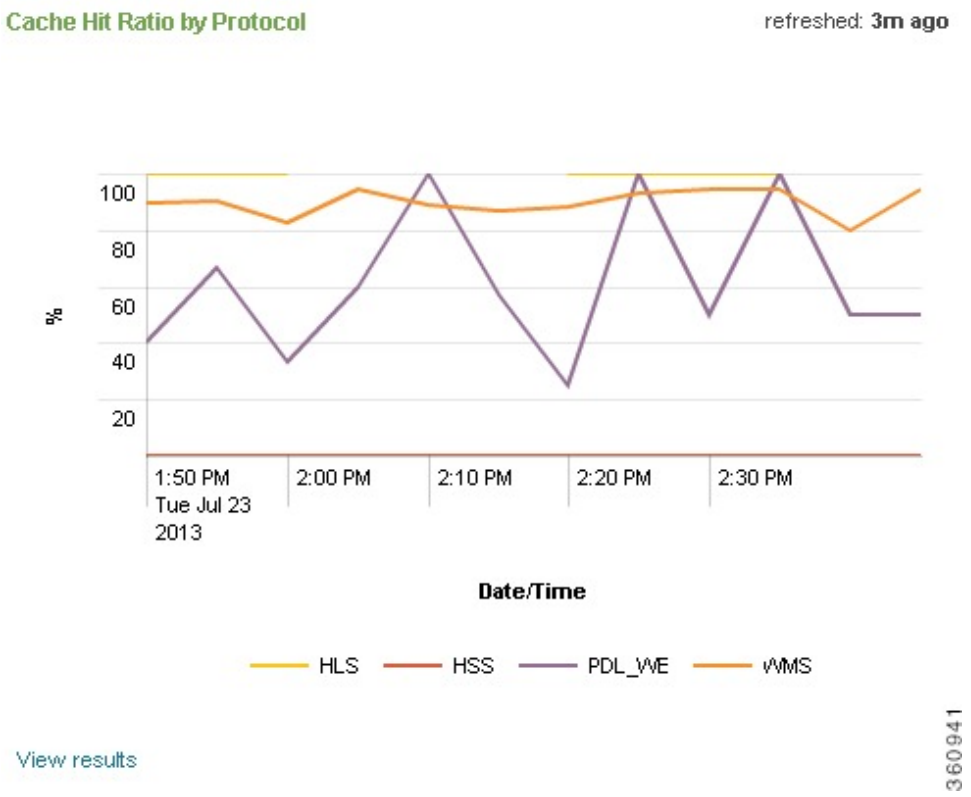


The following table describes the chart within this scorecard:

Table 14: Response Codes by Protocol Chart & Description

Chart	Description
Response Codes by Protocol	Illustrates the response codes for each protocol.
Chart Information	The information within this chart is a stacked bar graph with Count along the X-axis and Protocol along the Y-axis. The legends represent individual response codes.
Chart Formula	The formula used to derive the line graphs is: the count of individual response codes grouped by the response code and protocol.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Cache Hit Ratio by Protocol



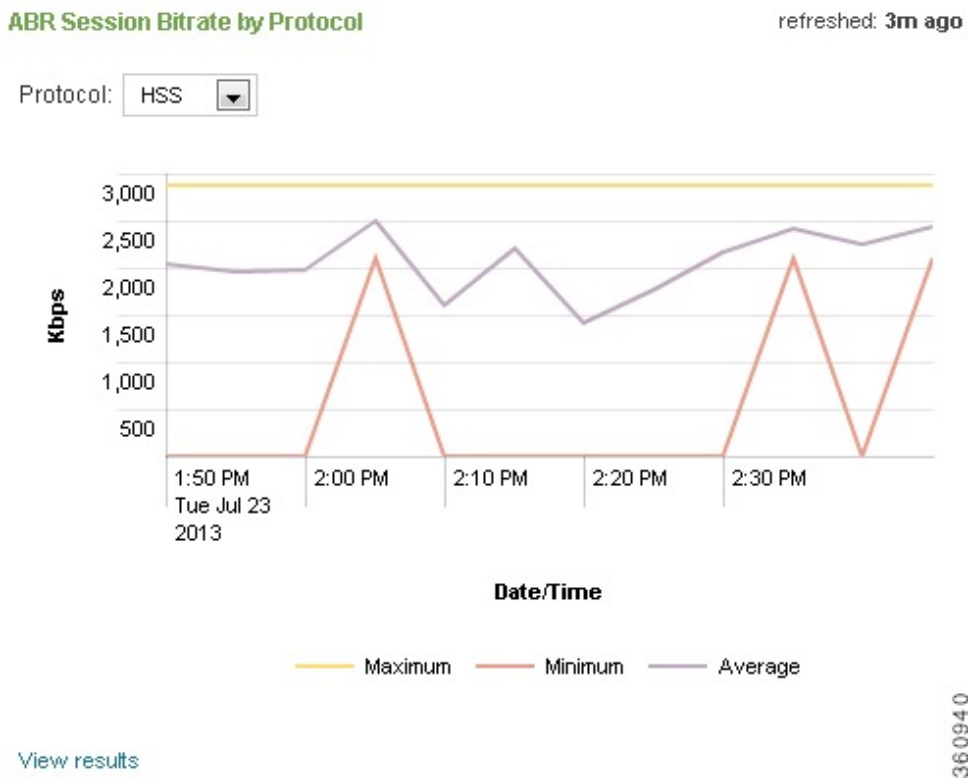
The following table describes the chart within this scorecard:

Table 15: Cache Hit Ratio by Protocol Chart & Description

Chart	Description
Cache Hit Ratio by Protocol	Illustrates the cache hit ratio for each protocol, for the specified time interval.
Chart Information	The information within this chart is shown in a line graph with Date/Time along the X-axis and cache hit ratio (%) along the Y-axis. The legends representing the graph are protocols.
Chart Formula	The formula used to derive the graph is: the percentage of cache hit over total requests grouped by the protocol.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Note Cache hit ratio for FMS will not be displayed in this chart as FMS logs do not contain caching information.

ABR Session Bitrate by Protocol



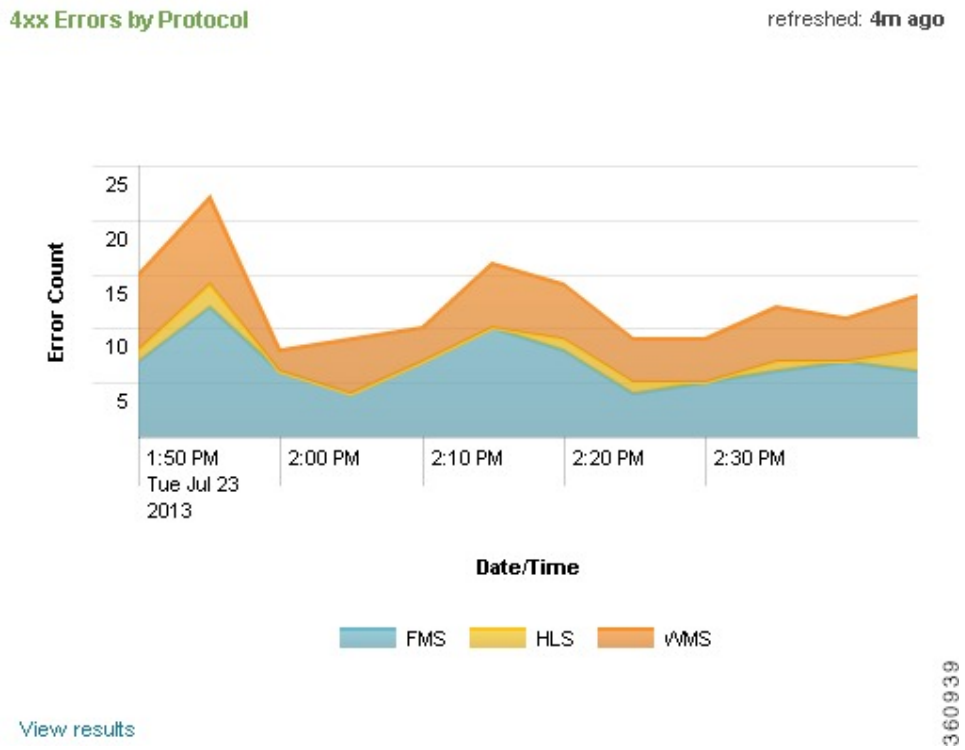
The following table describes the chart within this scorecard:

Table 16: ABR Session Bitrate by Protocol Chart & Description

Chart	Description
ABR Session Bitrate by Protocol	Provides HSS (HTTP smooth streaming), HLS (HTTP live streaming), and MobiTV average bitrate (Kbps). Click the Protocol drop-down list and select the respective protocol to choose HSS, HLS, and MobiTV.
Chart Information	The information within this chart is shown in a line graph with Date/Time along the X-axis and maximum, minimum, and average bitrate (Kbps) along the Y-axis. The legends representing the graph are maximum, minimum, and average.
Chart Formula	The formula used to derive the line graphs is: calculate the maximum, minimum, and average of bitrate, for the specified time interval.

Chart	Description
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

4xx Errors by Protocol



The following table describes the chart within this scorecard:

Table 17: 4xx Errors by Protocol Chart & Description

Chart	Description
4xx Errors by Protocol	Illustrates the number of 4xx errors for each protocol, for the specified time interval.
Chart Information	The information within this chart is shown in a stacked area graph with the Date/Time along the X-axis and the Error Count along the Y-axis. The legends representing the graph are protocol types.

Chart	Description
Chart Formula	The formula used to derive the graphs is: the count of 4xx errors in each protocol, for the specified time interval.
Chart Filters	This chart uses Time Range (Last 60 Minutes, Last 24 Hours, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Content

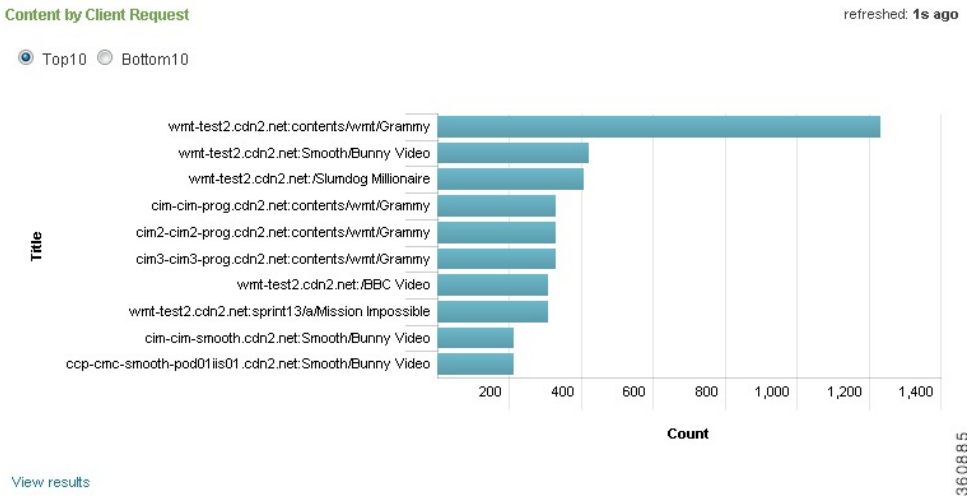
This tab displays charts that provides an overview of the top content, based on different dimensions such as content by client request, bytes transferred, and average ABR session bitrate. By default, the data for the previous day is displayed in the scorecard.

To access this tab, click **Home** > **Content**.

The following metrics are displayed here:

- Content by Client Request
- Content by Bytes Transferred
- Average ABR Session Bitrate by Content
- Top Content by Delivery Server
- Top Content by City
- Top Content by Client Type

Content by Client Request



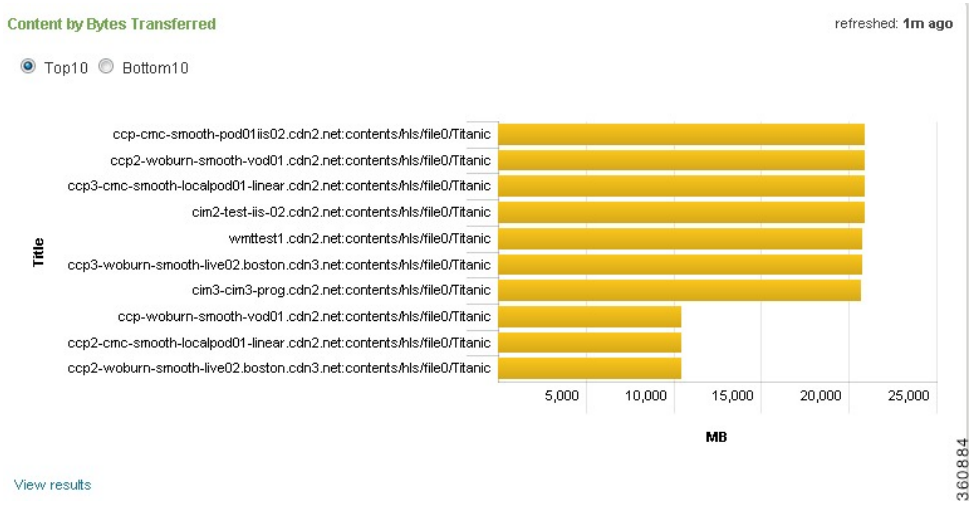
The following table describes the chart within this scorecard:

Table 18: Content by Client Request Chart & Description

Chart	Description
Content by Client Request	Illustrates the most/least popular content, based on the number of client requests received.
Chart Information	The information within this chart is shown in a bar graph with Count along the X-axis and Title along the Y-axis.
Chart Formula	The formula used to derive the graph is the most/least viewed content titles by client session count, per day.
Chart Filters	This chart uses Time Range (Previous day and Last 7 days), Delivery Server, Provider, Service Type (Live and VOD), Delivery Service, Resolution (HD and SD), and Genre, as filters.

To view the top 10 content by client request and the bottom 10 content by client request, click the respective radio buttons located above the chart.

Content by Bytes Transferred



The following table describes the chart within this scorecard:

Table 19: Content by Bytes Transferred Chart & Description

Chart	Description
Content by Bytes Transferred	Illustrates the most/least popular content, based on the download size.

Chart	Description
Chart Information	The information within this chart is shown in a bar graph as MB along the X-axis and Title along the Y-axis.
Chart Formula	The formula used to derive the graph is the most/least viewed content titles by bytes transferred to clients, per day.
Chart Filters	This chart uses Time Range (Previous day and Last 7 days), Delivery Server, Provider, Service Type (Live and VOD), Delivery Service, Resolution (HD and SD), and Genre, as filters.

Note To view the top 10 content by bytes transferred and the bottom 10 content by bytes transferred, click the respective radio buttons located above the chart.

Average ABR Session Bitrate by Content

The following table describes the information in the tabular column:

Table 20: Average ABR Session Bitrate by Content Table & Description

Table	Description
Average ABR Session Bitrate by Content	Illustrates the content delivered with highest/lowest bitrate.

Table	Description
Table Information	The information within this table are Title and Average bitrate.
Formula	The formula used is: the top/bottom content title by average bitrate.
Filters	This table uses Time Range (Previous day and Last 7 days), Delivery Server, Provider, Service Type (Live and VOD), Delivery Service, Resolution (HD and SD), and Genre, as filters.

Note To view the top 10 average ABR session bitrate by content and the bottom 10 average ABR session bitrate by content, click the respective radio buttons located above the chart.

Top Content by Delivery Server

360285

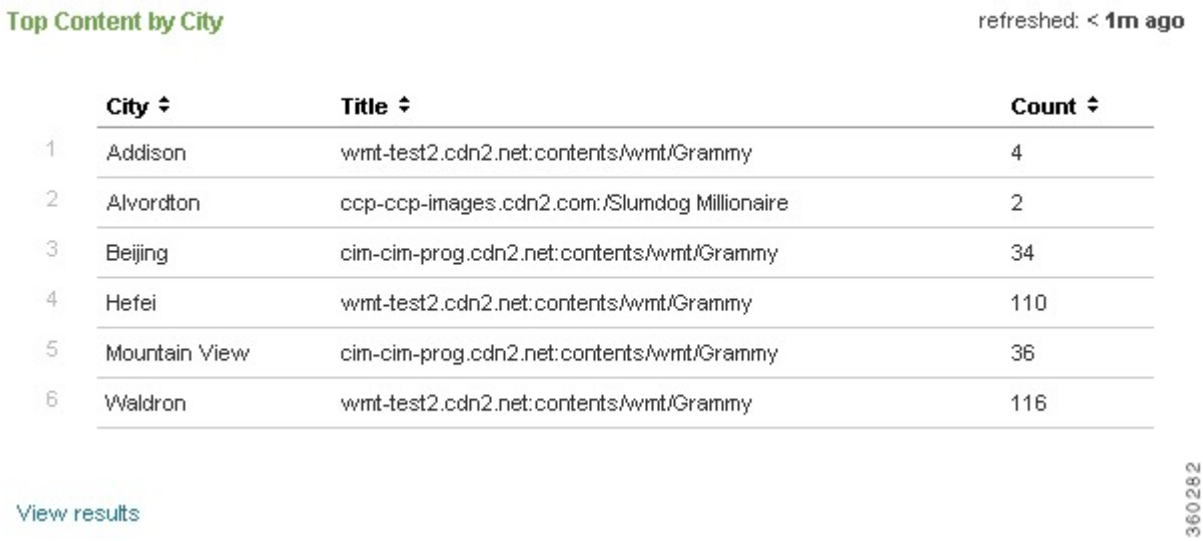
The following table describes the information in the tabular column:

Table 21: Top Content by Delivery Server Table & Description

Table	Description
Top Content by Delivery Server	Illustrates the most popular content served by each delivery server.
Table Information	The information within this table are Delivery Server, Title, and Count.
Formula	The formula used is: the top content title (based on count) by delivery server.

Table	Description
Filters	This table uses Time Range (Previous day and Last 7 days), Delivery Server, Provider, Service Type (Live and VOD), Delivery Service, Resolution (HD and SD), and Genre, as filters.

Top Content by City



The following table describes the information in the tabular column:

Table 22: Top Content by City Table & Description

Table	Description
Top Content by City	Illustrates the most popular content viewed in a city.
Table Information	The information within this table are City, Title, and Count.
Formula	The formula used is: the top content title (based on count) by city.
Filters	This table uses Time Range (Previous day and Last 7 days), Delivery Server, Provider, Service Type (Live and VOD), Delivery Service, Resolution (HD and SD), and Genre, as filters.

To view the list of viewers accessing ISP and Net Speed network, click the respective radio buttons located above the chart.

Note The city will be resolved only for public IPs. IPs which cannot be resolved by MaxMind will not be displayed.

Top Content by Client Type


Top Content by Client Type

refreshed: < 1m ago

	Client Type	Title	Count
1	NSPlayer/12.0.7600.16385	wmt-test2.cdn2.net:contents/wmt/Grammy	617
2	NSPlayer/12.0.7600.16385 WMFSDK/12.0	wmt-test2.cdn2.net:contents/wmt/Grammy	616
3	Mozilla/4.0	wmt-test2.cdn2.net:Smooth/Bunny Video	420
4	WMFSDK/12.0.7600.16385_WMPlayer/12.0.7600.16667	wmt-test2.cdn2.net:/BBC Video	309
5	MAC 8,0,246,0	ccp2-ccp2-images.cdn2.com:/Slumdog Millionaire	206
6	WIN 11,2,202,235	ccp2-cmo-smooth-pod01iis01.cdn2.net:/Slumdog Millionaire	206
7	Apple Mac OS X v10.6.7 CoreMedia v1.0.0.10J869	ccp2-woburn-smooth-vod01.cdn2.net:contents/hls/file0/Titanic	166
8	IE/7.0	ccp-woburn-smooth-live02.boston.cdn3.net:Smooth/Bunny Video	165
9	VLC/1.0.1_LibVLC/1.0.1	ccp-woburn-smooth-vod01.cdn2.net:contents/hls/file0/Titanic	165

View results

360640

The following table describes the information in the tabular column:

Table 23: Top Content by Client Type Table & Description

Table	Description
Top Content by Client Type	Illustrates the most popular content viewed in each client (players and browsers that is used to request the content).
Table Information	The information within this table are Client Type, Title, and Count.
Formula	The formula used is: the top content title (based on count) by client type.
Filters	This table uses Time Range (Previous day and Last 7 days), Delivery Server, Provider, Service Type (Live and VOD), Delivery Service, Resolution (HD and SD), and Genre, as filters.

Viewers

This tab displays charts that explains the viewer density, based on different parameters such as city, ISP, Net speed, session duration, and download size. By default, the data for the previous day is displayed in the scorecard.

To access this tab, click **Home** > **Viewers**.

The following metrics are displayed here:

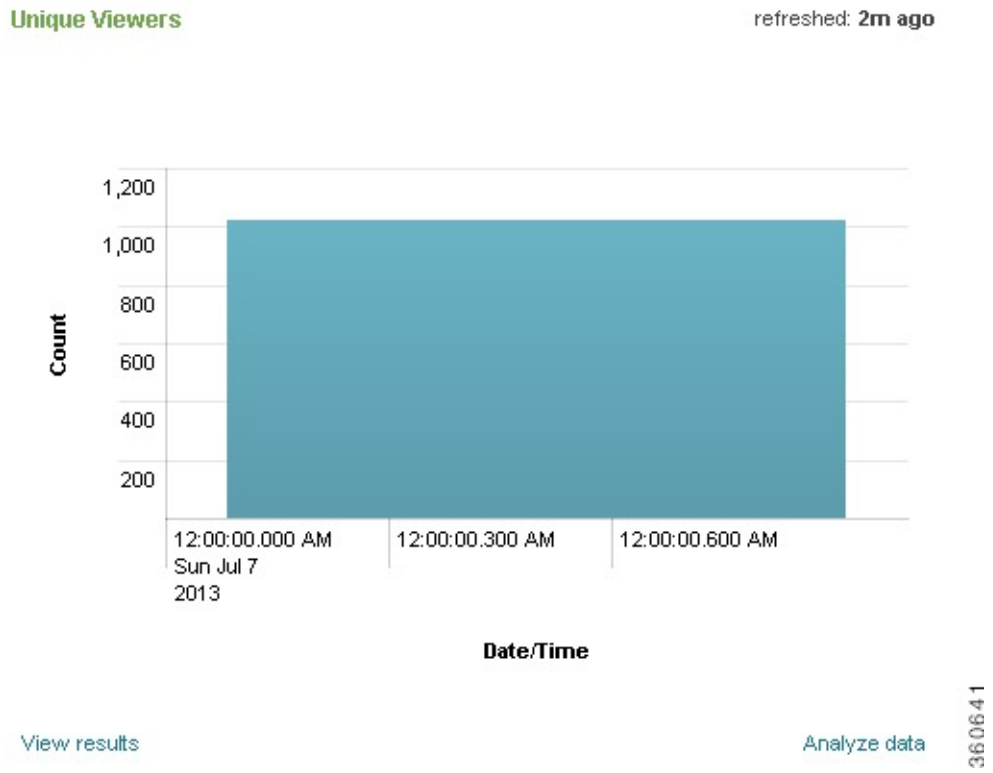
- Client Density by Number of Requests
- Unique Viewers
- Viewers by Client Type
- Viewers by City
- Viewers by ISP and Net Speed
- Viewers by Session Duration

Client Density by Number of Requests

This map displays all the client locations as points. The country in which the viewers are present will be highlighted. When you mouse hover the client location, the number of viewers from that particular location will be displayed.

Note The public IPs that are not resolved by MaxMind will be represented as '-' in the maps.

Unique Viewers



The following table describes the chart within this scorecard:

Table 24: Unique Viewers Chart & Description

Table	Description
Unique Viewers	Illustrates the number of unique viewers per day.
Chart Information	The information within this chart is shown in a column graph with the Date/Time along the X-axis and the unique viewer Count along the Y-axis.
Formula	The formula used to derive the graph is the total unique viewer, per day.
Filters	This chart uses Time Range (Previous Day, and Last 7 days), Delivery Server, Provider, and Delivery Service, as filters.

Viewers by Client Type


Viewers by Client Type

refreshed: 2m ago

	Client Type	Count
1	Core Media	484
2	Internet Explorer 7	472
3	MAC Version 8	484
4	Firefox 4	510
5	NS Player	685
6	NS Player WMFSDK	686
7	VLC Media Player	476
8	Windows Media Player 11	982
9	WMFSDK	765

View results

Analyze data

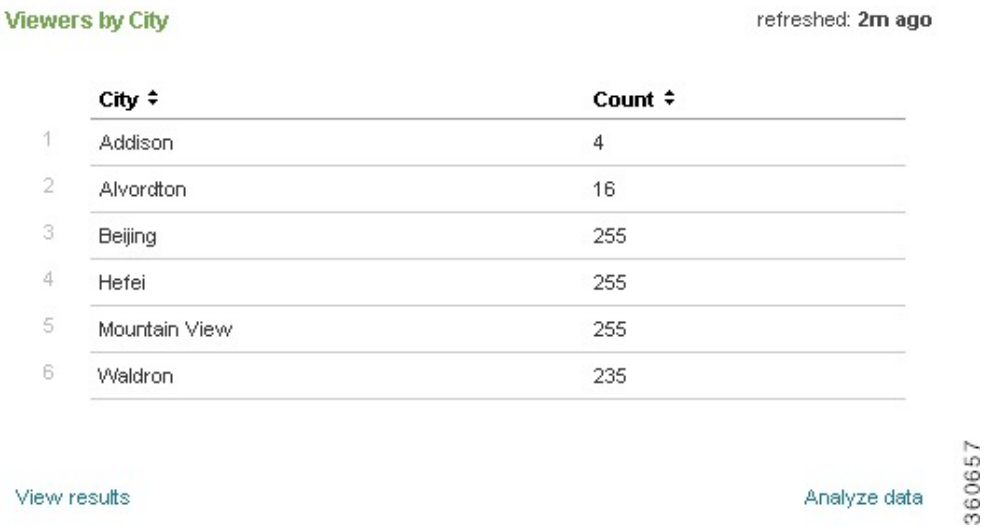
360658

The following table describes the chart within this scorecard:

Table 25: Viewers by Client Type Table & Description

Table	Description
Viewers by Client Type	Illustrates the number of viewers accessing the network through each client.
Table Information	The information within this table are Client Type and Count.
Formula	The formula used is: unique viewer by client type and request count.
Filters	This chart uses Time Range (Previous Day, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Viewers by City



The following table describes the chart within this scorecard:

Table 26: Viewers by City Table & Description

Table	Description
Viewers by City	Illustrates the number of viewers accessing the network in each city.
Table Information	The information within this table are City and Count.
Formula	The formula used is: the number of unique viewers in each city.
Filters	This chart uses Time Range (Previous Day, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Note The city will be resolved only for public IPs. IPs which cannot be resolved by MaxMind will not be displayed.

Viewers by ISP and Net Speed

The following table describes the chart within this scorecard:

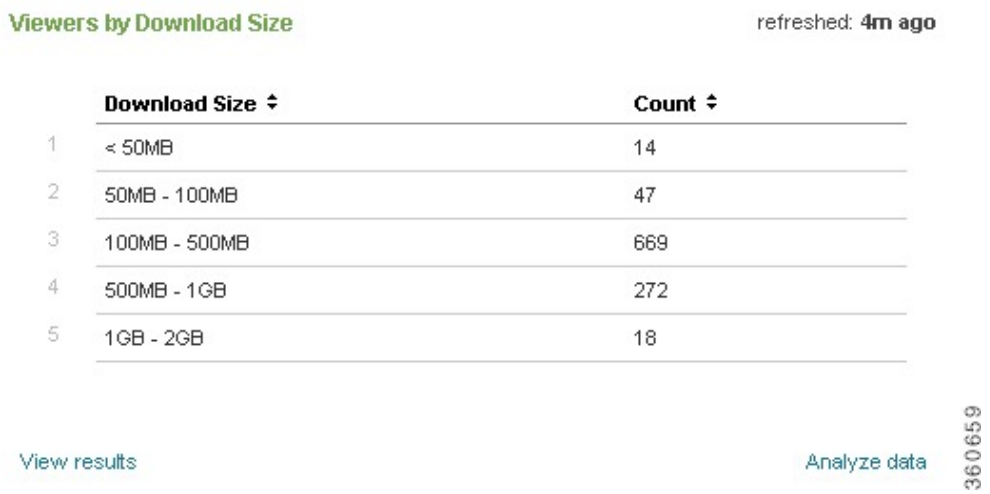
Table 27: Viewers by ISP and Net Speed Table & Description

Table	Description
Viewers by ISP and Net Speed	Illustrates the number of viewers accessing the network, grouped by Internet Service Provider (ISP) or Net Speed.
Table Information	The information within this table are ISP or Net Speed and Count.
Formula	The formula used is: the number of unique viewers grouped by client ISP or Net Speed.
Filters	This chart uses Time Range (Previous Day, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

To view the list of viewers accessing ISP and Net Speed network, click the respective radio buttons located above the chart.

Note Other than public IPs, "unknown" value will be displayed.

Viewers by Download Size



The following table describes the chart within this scorecard:

Table 28: Viewers by Download Size Table & Description

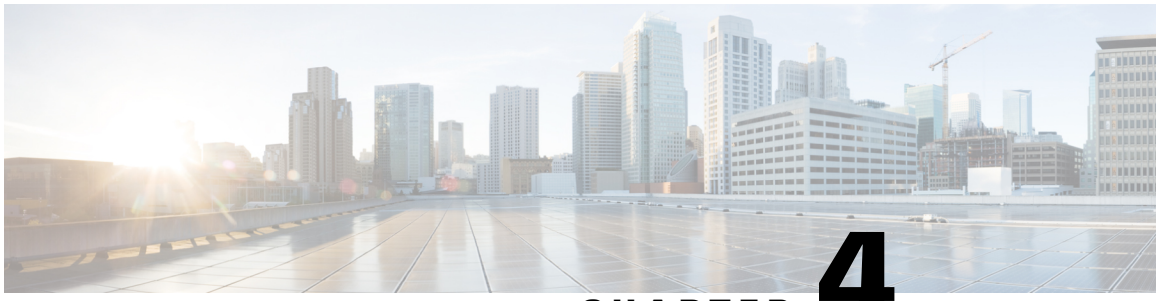
Table	Description
Viewers by Download Size	Illustrates the number of viewers, based on the download size.
Table Information	The information within this table are Download Size and Count.
Formula	The formula used is: the number of viewers bucketed by the download size in MB.
Filters	This chart uses Time Range (Previous Day, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.

Viewers by Session Duration

The following table describes the chart within this scorecard:

Table 29: Viewers by Session Duration Table & Description

Table	Description
Viewers by Session Duration	Illustrates the number of viewers, based on session duration.
Table Information	The information within this table are Average Session Duration (minutes) and Count.
Formula	The formula used is: the number of unique viewers bucketed by the average session duration.
Filters	This chart uses Time Range (Previous Day, and Last 7 days), Delivery Server, Provider, and Delivery Service as filters.



CHAPTER 4

Analytics

Analytics Overview

This section provides an overview of the VDS-SM Analytics, which provides the ability to view and analyze data that are collected about trends, reports, content, and sessions in textual and graphical form.

Data is pushed from various streaming devices to the Splunk Universal Forwarder, and then to the VDS-SM. The data available is used to provide a multitude of historical search capabilities. Data is gathered using predefined indexing metrics, designed to provide data that is monitored by service provider operators. The data output is viewed in the form of a dashlet.

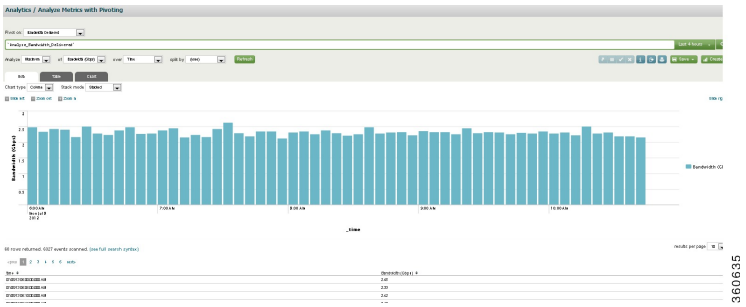
Analyze Metrics with Pivoting

This feature allows the CDN Operators to analyze the data at a granular level. The difference between the Analyze data option on individual charts and generic pivoting is that, in pivoting, you need to select an option to start the analysis. You can analyze the data for the following:

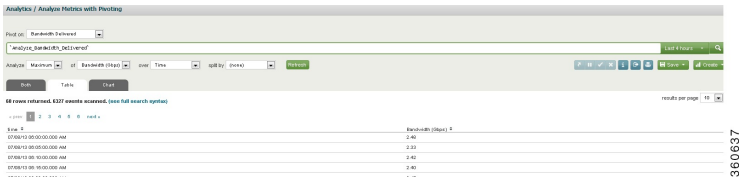
- Bandwidth Delivered
- Cache Efficiency
- Concurrent Active Sessions
- GigaBytes Delivered
- Requests
- Response Codes
- Storage Usage
- Viewers

You can view the data in the following ways:

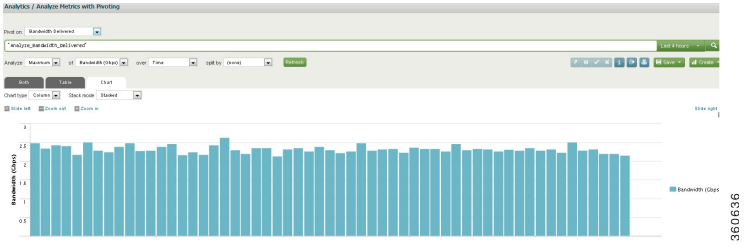
- By clicking the **Both** tab, the data will be displayed, in a tabular column and chart.



- By clicking the **Table** tab, the data will be displayed in a tabular column.



- By clicking the **Chart** tab, the data will be displayed in a chart/graph.



You can view the same data in different charts and stack modes. Click the **Chart type** and **Stack mode** drop-down lists respectively, and select the chart and stack mode of your choice. The different chart types are column, bar, line, area, and pie. The different types of stack modes are stacked, none, and 100% stacked.

Note When you select an option other than Time in the **over** drop-down list and select none in the **split by** drop-down list, additional drop-down lists such as top/bottom and the number of results to be plotted are displayed.

To access this feature, perform the following steps:

Step 1 Select **Analytics** > **Analyze Metrics with Pivoting**.

Step 2 From the **Pivot on:** drop-down list, select the category for which you need to analyze the data.

Step 3 From the **Analyze**, **of**, **over**, and **split by** drop-down lists, select the required options.

Trends

This feature allows you to view the historical data (more than 7 days), in a graph and tabular column. VDS-SM Analytics gather historical data from different perspectives, such as the following:

- Network
- Streaming
- Viewers
- Content
- Billing

When you click each of these categories, the respective subcategories are expanded. On further expanding the subcategories, the respective dashlets are listed.

When each of these dashlets are selected, the corresponding charts and data (in a tabular column) are displayed on the right pane. When you click **View results** option below the charts, the log information corresponding to the dashlet is displayed.

Note In the search field, which is located in the left pane, enter the dashlet name or part of the dashlet name as a search string. This will display the receptive dashlet names.

Network

Network trends dashboard provides an historical information on volume, caching, request, and response of the managed CDN network.

To access this feature, perform the following:

1. From the main page, click **Analytics** > **Trends**.

2. From the tree view, which appears in the left pane, select **Network**.

The following subcategories are displayed in Network:

Volume

Caching

Request

Response

Volume

This category includes data and charts for Throughput, Volume of Data Delivered, Delivery Services by Bytes Delivered, and Origin/Ingest Volume.

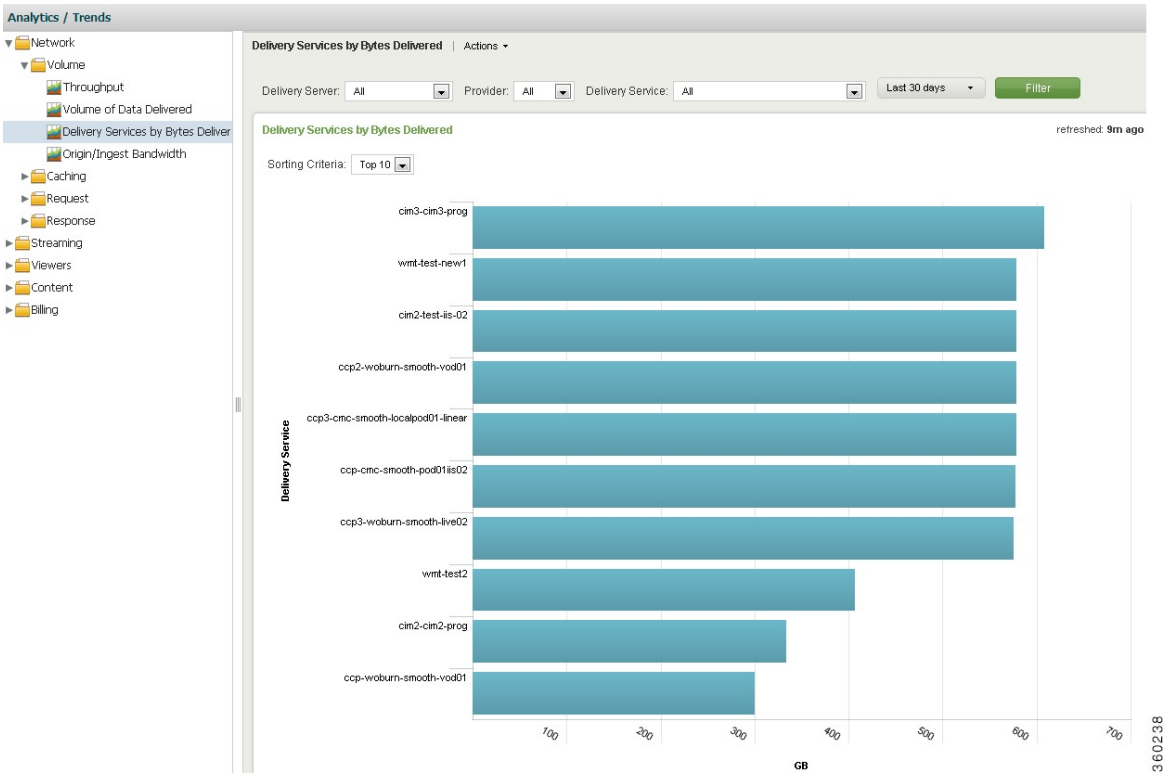
Throughput

For details, see Throughput , on page 28

Volume of Data Delivered

For details, see Volume Delivered by Protocol , on page 37

Delivery Services by Bytes Delivered



The following table describes the chart within this dashlet:

Table 30: Delivery Services by Bytes Delivered Chart & Description

Chart	Description
Delivery Services by Bytes Delivered	Illustrates the top delivery services, based on the content delivered, for the specified time interval.
Chart Information	The information within this chart is a bar graph with the bytes delivered in GB along the X-axis and Delivery Service along the Y-axis.
Formula	The formula used to derive the graph is: Top 'n' delivery services by total bytes delivered.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

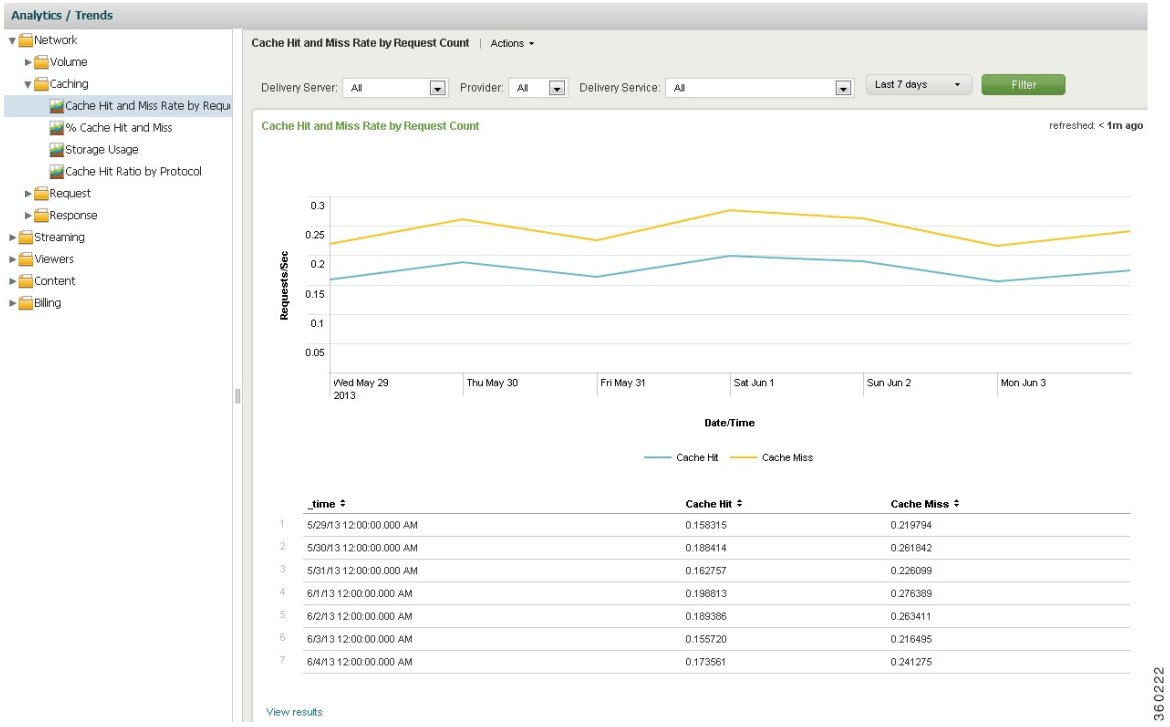
You can also view the top delivery services, such as top 10 and top 20, by clicking the **Sorting Criteria** drop-down list.

Origin/Ingest Volume
For details, see Origin/Ingest Volume, on page 32

Caching

This category includes the data and charts for Cache Hit and Miss Rate by Request Count, % Cache Hit and Miss, Storage Usage, and Cache Hit Ratio by Protocol.

Cache Hit and Miss Rate by Request Count

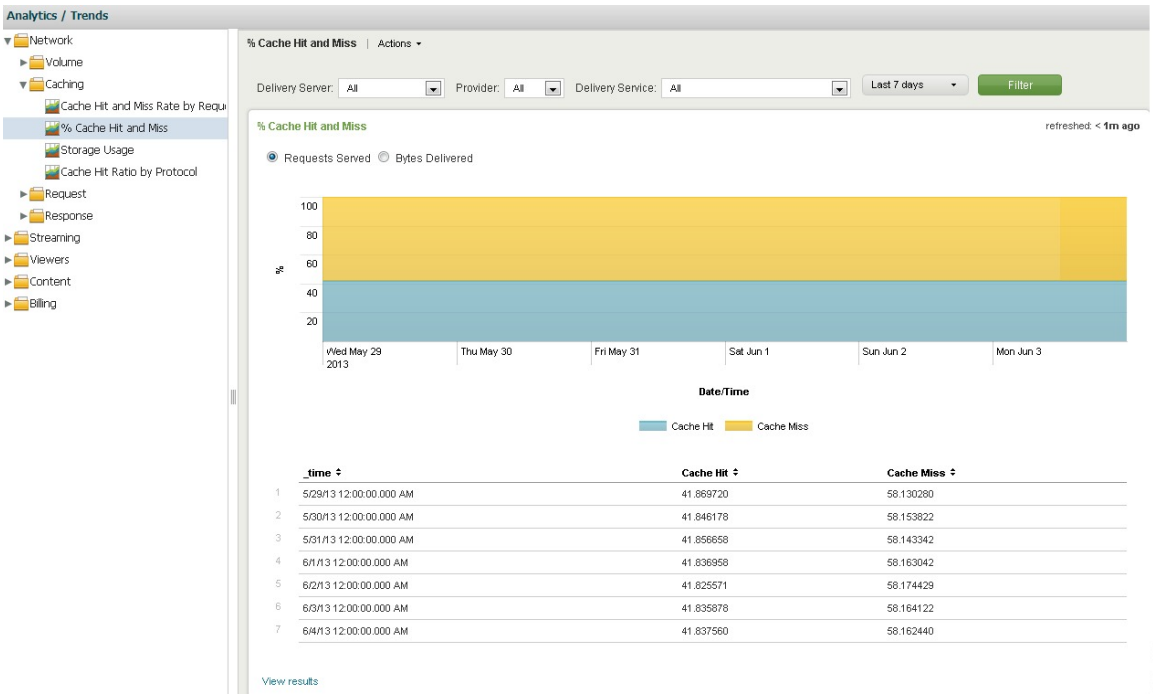


The following table describes the chart within this dashlet:

Table 31: Cache Hit and Miss Rate by Request Count Chart & Description

Chart	Description
Cache Hit and Miss Rate by Request Count	Illustrates the rate of cache hit and miss, for the specified time interval.
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and Requests per Second along the Y-axis. The legends are Cache Hit and Cache Miss.
Formula	The formula used to derive the graph is: the rate of cache hit and cache miss requests per second.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

% Cache Hit and Miss



The following table describes the chart within this dashlet:

Table 32: % Cache Hit and Miss Chart & Description

Chart	Description
% Cache Hit and Miss	Illustrates the percentage of cache hits and cache miss, based on the number of requests served and total bytes delivered, for the specified time interval.
Chart Information	The information within this chart is a stacked area graph with Date/Time along the X-axis and Cache Hit and Cache Miss percentage along the Y-axis. The legends are Cache Hit and Cache Miss.
Formula	The formula used to derive the requests served graph is: percentage of cache hit and cache miss over total requests. The formula used to derive the bytes delivered graph is: percentage of cache hit bytes and cache miss bytes over total bytes delivered.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

You can view the request served and bytes delivered by clicking the respective radio buttons.

Storage Usage

For details, see Storage Usage, on page 35

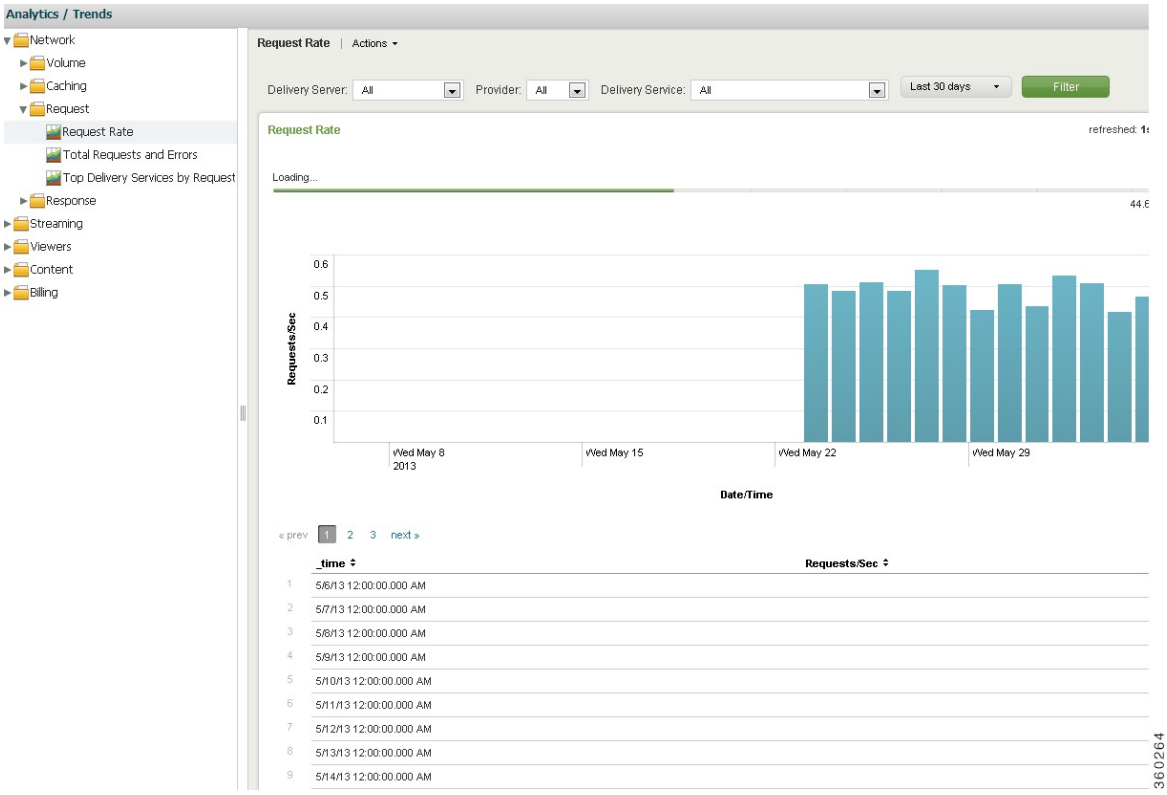
Cache Hit Ratio by Protocol

For details, see Cache Hit Ratio by Protocol, on page 40

Request

This category includes data and charts for Request Rate, Total Requests and Errors, and Top Delivery Services by Request Count.

Request Rate

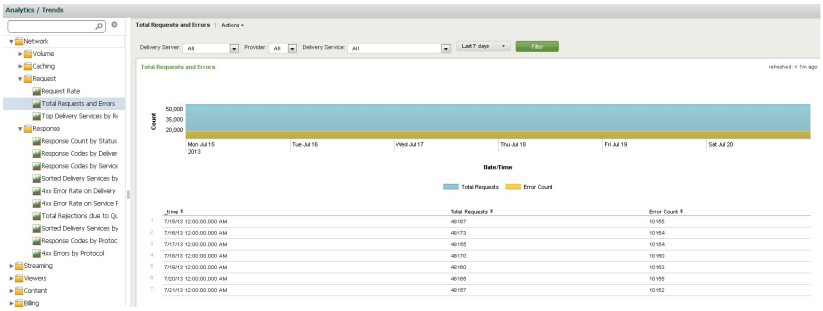


The following table describes the chart within this dashlet:

Table 33: Request Rate Chart & Description

Chart	Description
Request Rate	Illustrates the number of requests per second, for the specified time interval.
Chart Information	The information within this chart is a column graph with Date/Time along the X-axis and Requests per Second along the Y-axis.
Formula	The formula used to derive the graph is: the number of requests per second.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

Total Requests and Errors



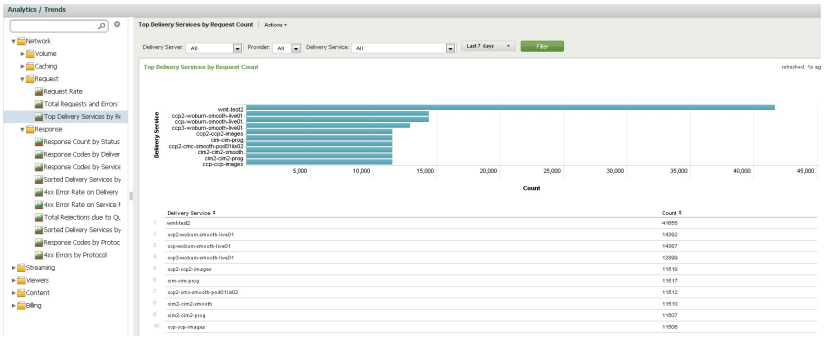
360893

The following table describes the chart within this dashlet:

Table 34: Total Requests and Errors Chart & Description

Chart	Description
Total Requests and Errors	Illustrates the total requests and the number of errors from the total requests, for the specified time interval.
Chart Information	The information within this chart is an area graph with Date/Time along the X-axis and the requests/error Count along the Y-axis. The legends are Total Requests and Error Count.
Formula	The formula used to derive the graph is: the total number of requests and errors (requests with status codes 4xx or 5xx).
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

Top Delivery Services by Request Count



360892

The following table describes the chart within this dashlet:

Table 35: Top Delivery Services by Request Count Chart & Description

Chart	Description
Top Delivery Services by Request Count	Illustrates the top delivery services by request count, for the specified time interval.
Chart Information	The information within this chart is a bar graph with request count along the X-axis and the top Delivery Services along the Y-axis.
Formula	The formula used to derive the graph is: the top 10 delivery services by the number of requests received by them.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

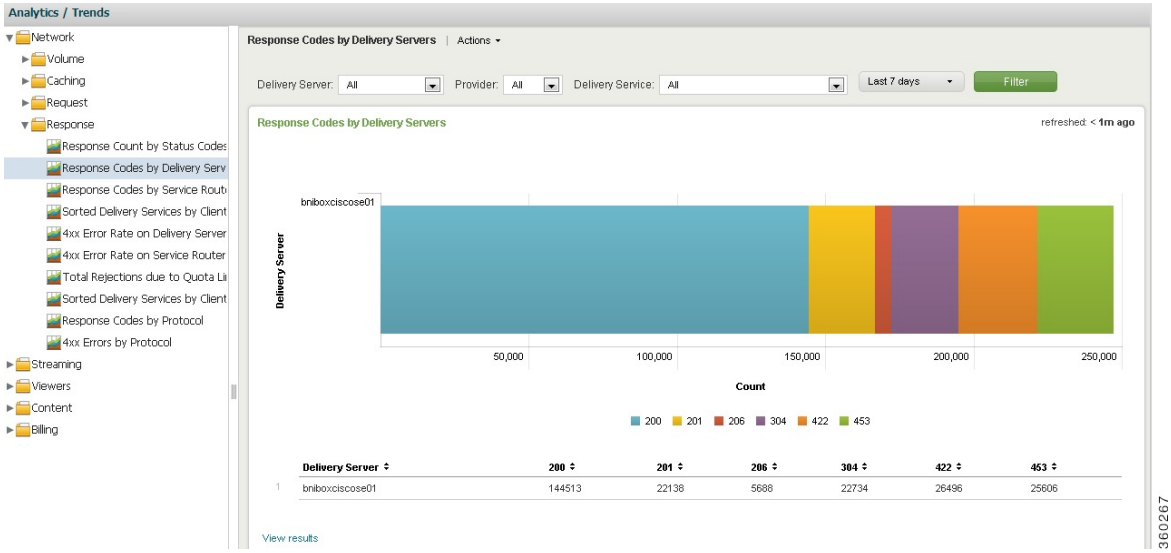
Response

This category includes data and charts for Response Count by Status Codes, Response Codes by Delivery Servers, Response Codes by Service Routers, Sorted Delivery Services by Client Errors on Delivery Servers, 4xx Error Rate on Delivery Servers, 4xx Error Rate on Service Routers, Total Rejections due to Quota Limits, Sorted Delivery Services by Client Errors on Service Routers, Response Codes by Protocol, and 4xx Errors by Protocol.

Response Count by Status Codes

For details, see Response Status Codes, on page 34

Response Codes by Delivery Servers

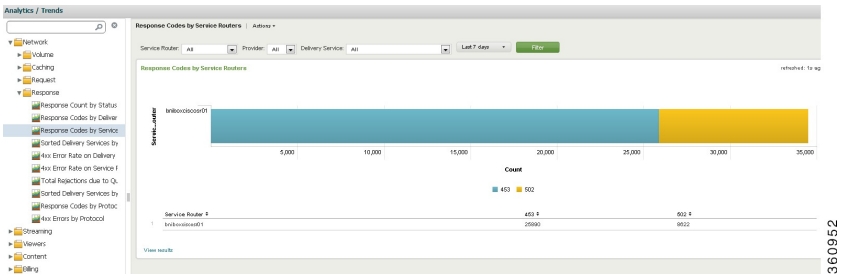


The following table describes the chart within this dashlet:

Table 36: Response Codes by Delivery Servers Chart & Description

Chart	Description
Response Codes by Delivery Servers	Illustrates the responses that are grouped by status codes (such as success, client error, and server error: status of a request), for a given delivery server.
Chart Information	The information within this chart is a stacked bar graph with response count along the X-axis and the Delivery Server along the Y-axis. The legends are the status codes.
Formula	The formula used to derive the graph is: the number of responses grouped by the response codes for each delivery server.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

Response Codes by Service Routers

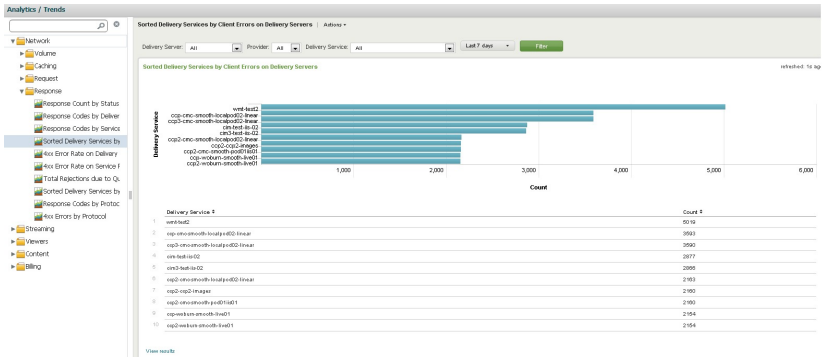


The following table describes the chart within this dashlet:

Table 37: Response Codes by Service Routers Chart & Description

Chart	Description
Response Codes by Service Routers	Illustrates the responses that are grouped by status codes (client and server errors), for a given service router, for the specified time interval.
Chart Information	The information within this chart is a stacked area graph with response code Count along the X-axis and Service Router along the Y-axis.
Formula	The formula used to derive the graph is: the number of responses grouped by the response codes for each service router.
Chart Filters	This chart uses Service Router, Provider, Delivery Service and the Time Range Picker as filters.

Sorted Delivery Services by Client Errors on Delivery Servers

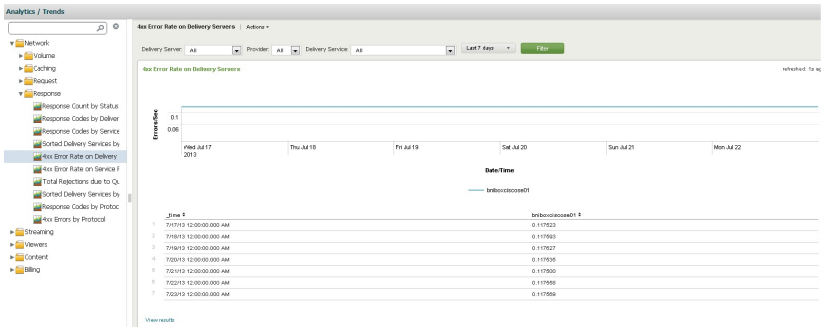


The following table describes the chart within this dashlet:

Table 38: Sorted Delivery Services by Client Errors on Delivery Servers Chart & Description

Chart	Description
Sorted Delivery Services by Client Errors on Delivery Servers	Illustrates the top 10 delivery services by client errors.
Chart Information	The information within this chart is a bar graph with error Count along the X-axis and Delivery Service along the Y-axis.
Formula	The formula used to derive the graph is: the top 10 delivery services by the number of 4xx errors.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

4xx Error Rate on Delivery Servers

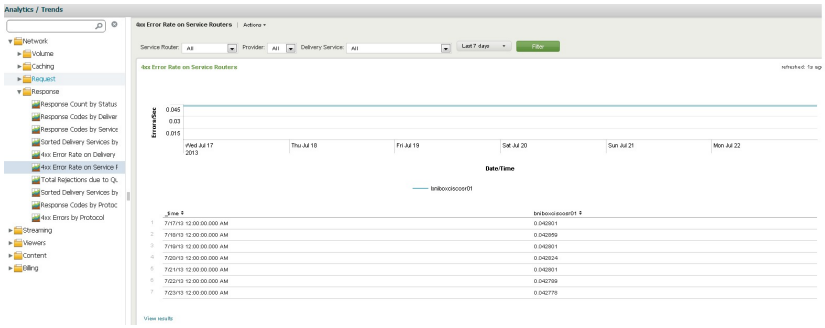


The following table describes the chart within this dashlet:

Table 39: 4xx Error Rate on Delivery Servers Chart & Description

Chart	Description
4xx Error Rate on Delivery Servers	Illustrates the number of 4xx errors per second for each delivery server, for the specified time interval.
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and 4xx Errors per Second along the Y-axis. The legends are Delivery Servers.
Formula	The formula used to derive the graph is: the number of errors per second for each delivery server.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

4xx Error Rate on Service Routers

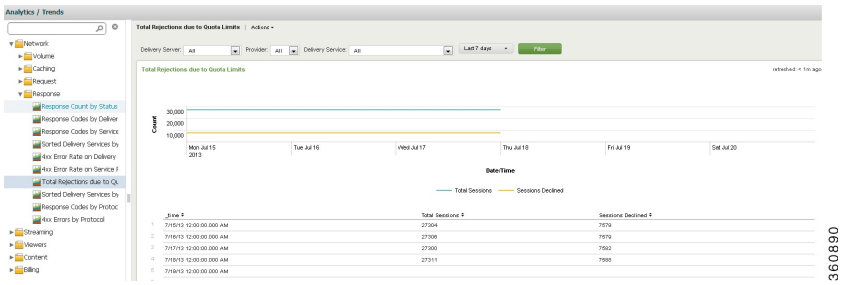


The following table describes the chart within this dashlet:

Table 40: 4xx Error Rate on Service Routers Chart & Description

Chart	Description
4xx Error Rate on Service Routers	Illustrates the number of 4xx errors per second for each service router, for the specified time interval.
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and Errors per Second along the Y-axis. The legends are Service Routers.
Formula	The formula used to derive the graph is: the number of errors per second for each service router.
Chart Filters	This chart uses Service Router, Provider, Delivery Service and the Time Range Picker as filters.

Total Rejections due to Quota Limits

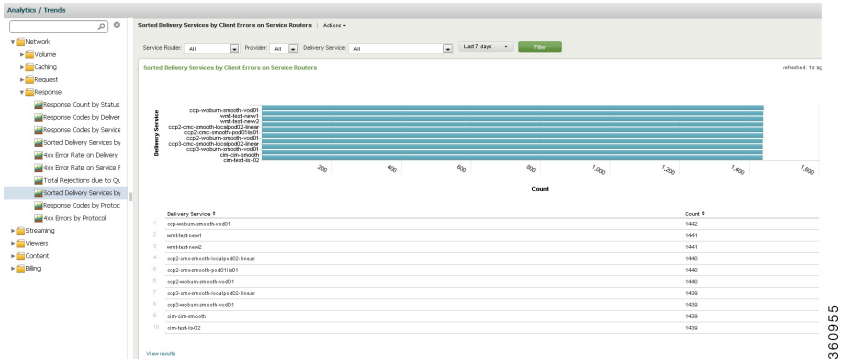


The following table describes the chart within this dashlet:

Table 41: Total Rejections due to Quota Limits Chart & Description

Chart	Description
Total Rejections due to Quota Limits	Illustrates the number of sessions rejected due to quota limits, for the specified time interval.
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and Total Sessions and Sessions Rejected along the Y-axis. The legends are Total Sessions and Sessions Declined.
Formula	The formula used to derive the graph is: total requests and requests with response code 453 or 499 plotted over time.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

Sorted Delivery Services by Client Errors on Service Routers



The following table describes the chart within this dashlet:

Table 42: Sorted Delivery Services by Client Errors on Service Routers Chart & Description

Chart	Description
Sorted Delivery Services by Client Errors on Service Routers	Illustrates the top 10 delivery services by client errors on service routers.

Chart	Description
Chart Information	The information within this chart is a bar graph with error Count along the X-axis and Delivery Services along the Y-axis.
Formula	The formula used to derive the graph is: top 10 delivery services by the number of 4xx errors occurring at the service router.
Chart Filters	This chart uses Service Router, Provider, Delivery Service and the Time Range Picker as filters.

Response Codes by Protocol

For details, see Response Codes by Protocol, on page 39

4xx Errors by Protocol

For details, see 4xx Errors by Protocol, on page 43

Streaming

Streaming trends dashboard provides an historical information on sessions and ABR of the managed CDN network.

To access this feature, perform the following:

1. From the main page, click **Analytics** > **Trends**.

2. From the tree view, which appears in the left pane, select **Streaming**.

The following subcategories are displayed in Streaming:

Sessions

ABR

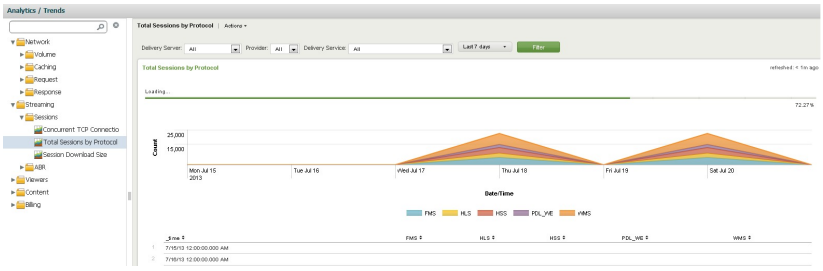
Sessions

This category includes data and charts for Concurrent Active Sessions, Total Sessions by Protocol, and Session Download Size.

Concurrent Active Sessions

For details, see Concurrent Active Sessions

Total Sessions by Protocol

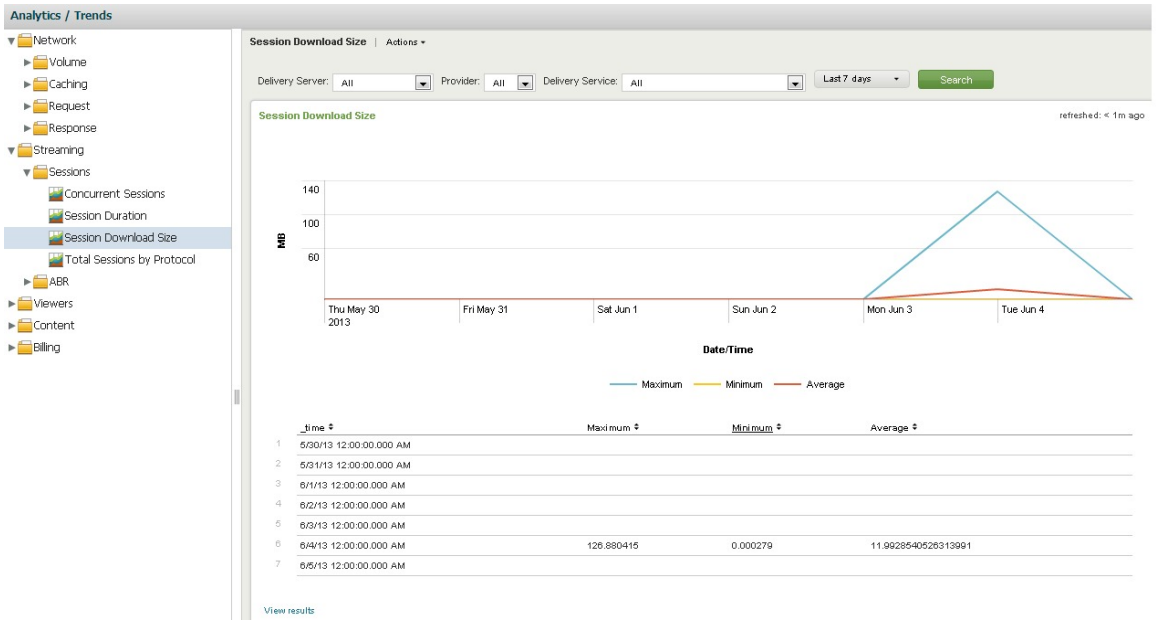


The following table describes the chart within this dashlet:

Table 43: Total Sessions by Protocol Chart & Description

Chart	Description
Total Sessions by Protocol	Illustrates the number of sessions by protocol, for the specified time interval.
Chart Information	The information within this chart is a stacked area graph with Date/Time along the X-axis and FMS, HLS, HSS, PDL_WE, and WMS Count along the Y-axis. The legends are FMS, HLS, HSS, PDL_WE, and WMS.
Formula	The formula used to derive the graph is: number of sessions grouped by protocol.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

Session Download Size



The following table describes the chart within this dashlet:

Table 44: Session Download Size Chart & Description

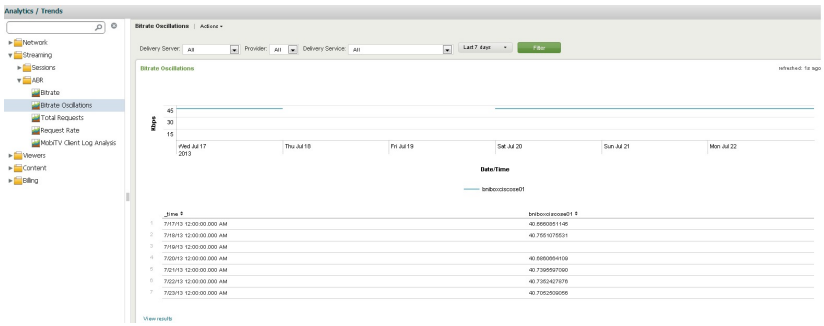
Chart	Description
Session Download Size	Illustrates the maximum, minimum, and average bytes delivered per session, for the specified time interval.

Chart	Description
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and the Maximum, Minimum, and Average download size in MB along the Y-axis. The legends are Maximum, Minimum, and Average.
Formula	The formula used to derive the graph is: the maximum, minimum, and average bytes delivered in MB plotted over time.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

ABR
Bitrate

For details, see ABR Session Bitrate by Protocol

Bitrate Oscillations

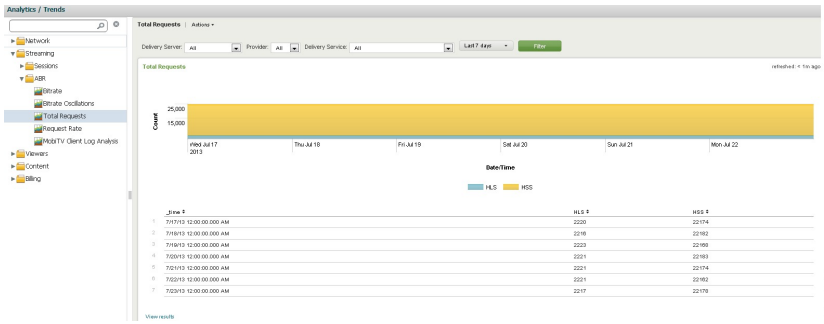


The following table describes the chart within this dashlet:

Table 45: Bitrate Oscillations Chart & Description

Chart	Description
Bitrate Oscillations	Illustrates the number of bitrate shifts per session, for the specified time interval.
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and bitrate oscillation in Kbps along the Y-axis.
Formula	The formula used to derive the graph is: bitrate shifts over time.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

Total Requests

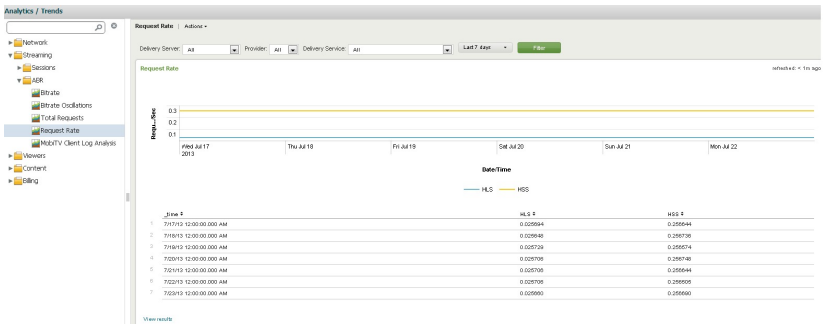


The following table describes the chart within this dashlet:

Table 46: Total Requests Chart & Description

Chart	Description
Total Requests	Illustrates the number of requests by traffic type (only ABR), for the specified time interval.
Chart Information	The information within this chart is a stacked area graph with Date/Time along the X-axis and the total request Count along the Y-axis. The legends are HLS, MobiTV, and HSS.
Formula	The formula used to derive the graph is: the number of requests per ABR protocol.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

Request Rate



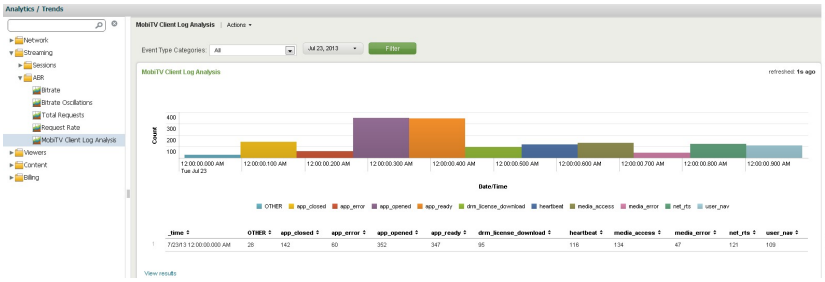
The following table describes the chart within this dashlet:

Table 47: Request Rate Chart & Description

Chart	Description
Request Rate	Illustrates the number of requests per second for each traffic type (HLS, HSS and MobiTV), for the specified time interval.

Chart	Description
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and the Requests per Second along the Y-axis. The legends are HLS, MobiTV, and HSS.
Formula	The formula used to derive the graph is: the number of requests per second for each traffic type of ABR protocol.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

MobiTV Client Log Analysis



The following table describes the chart within this dashlet:

Table 48: MobiTV Client Log Analysis Chart & Description

Chart	Description
MobiTV Client Log Analysis	Illustrates the number of MobiTV client log events per category, for the specified time interval.
Chart Information	The information within this chart is a column graph with Date/Time along the X-axis and the MobiTV client event Count along the Y-axis. The legends are MobiTV Client events.
Formula	The formula used to derive the graph is: the number of events for the specified event category split by events over time.
Chart Filters	This chart uses Event Type Categories and Time Range Picker as filters.

Viewers

Viewers trends dashboard provides an historical information on the number of unique viewers, viewers by client type, viewer density by location, top viewers, viewers by session duration, viewers by ISP and Net speed, viewers by protocol, and viewers by download size on the managed CDN network.

To access this feature, perform the following:

1. From the main page, click **Analytics** > **Trends**.

2. From the tree view, which appears in the left hand pane, select **Viewers**.

Number of Unique Viewers

For details, see Unique Viewers, on page 51

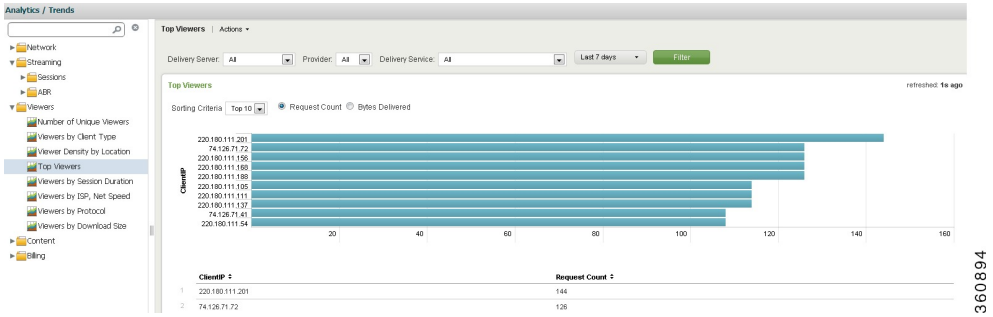
Viewers by Client Type

For details, see Viewers by Client Type, on page 52

Viewer Density by Location

For details, see Client Density by Number of Requests

Top Viewers



The following table describes the chart within this dashlet:

Table 49: Top Viewers Chart & Description

Chart	Description
Top Viewers	Illustrates the top viewers by total bytes delivered and request count, for a specified time interval.
Chart Information	The information within this chart is a bar graph with the Request Count/Bytes Delivered along the X- axis and Client IP address along the Y-axis.
Formula	The formula used to derive the graph is: top 'n' viewers of requests and bytes delivered.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

You can view the top viewers, such as top 10 and top 20, by selecting the respective options from the **Sorting Criteria** drop-down list. You can also view the request count and bytes delivered by clicking the respective radio buttons.

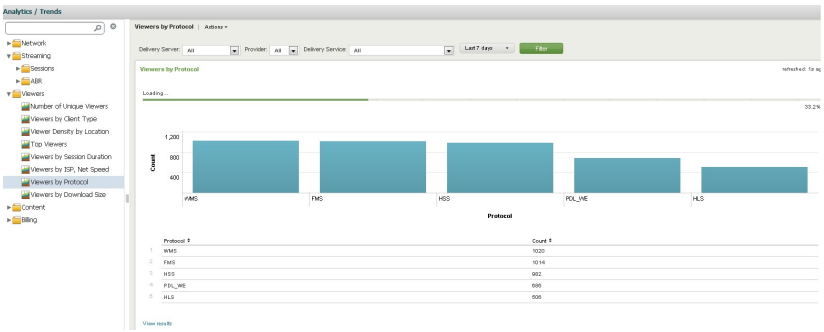
Viewers by Session Duration

For details, see Viewers by Session Duration, on page 56

Viewers by ISP, Net Speed

For details, see Viewers by ISP and Net Speed, on page 54

Viewers by Protocol



The following table describes the chart within this dashlet:

Table 50: Viewers by Protocol Chart & Description

Chart	Description
Viewers by Protocol	Illustrates the number of viewers per protocol, for the specified time interval.
Chart Information	The information within this chart is a column graph with Protocol along the X-axis and viewer Count along the Y-axis.
Formula	The formula used to derive the graph is: number of viewers grouped by protocol.
Chart Filters	This chart uses Delivery Server, Provider, Delivery Service and the Time Range Picker as filters.

Viewers by Download Size

For details, see Viewers by Download Size, on page 55

Content

Content trends dashboard provides an historical information on content by client requests, content by bytes transferred, top content by delivery server, average ABR session bitrate by content, top content by city, and top content by client type on the managed CDN network.

To access this feature, perform the following:

1. From the main page, click **Analytics** > **Trends**.

2. From the tree view, which appears in the left pane, select **Content**.

Content by Client Requests

For details, see Content by Client Request, on page 44

Content by Bytes Transferred

For details, see Content by Bytes Transferred, on page 45

Top Content by Delivery Server

For details, see Top Content by Delivery Server, on page 47

Average ABR Session Bitrate by Content

For details, see Average ABR Session Bitrate by Content, on page 46

Top Content by City

For details, see Top Content by City, on page 48

Top Content by Client Type

For details, see Top Content by Client Type, on page 49

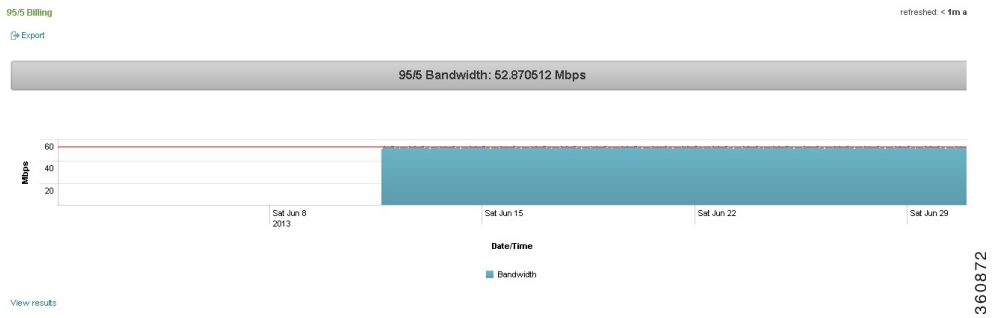
Billing

Billing trends dashboard provides an historical information on 95/5 billing on the managed CDN network.

To access this feature, perform the following:

1. From the main page, click **Analytics** > **Trends**.
2. From the tree view, which appears in the left hand pane, select **Billing**.

95/5 Billing



The following table describes the chart within this dashlet:

Table 51: 95/5 Billing Chart & Description

Chart	Description
95/5 Billing	Illustrates the billing data of previous months, which uses the 95/5 billing method.
Chart Information	The information within this chart is an area graph with Date/time along the X-axis and Bandwidth in Mbps along Y-axis.
Formula	The formula used to derive this is: The average bandwidth from SR Snapshot log by hour. The red line is the 95/5 high bandwidth within the whole month.
Chart Filters	This chart uses Month and Delivery Service as filters.

Billing Functionalities

By default, billing will be automatically generated daily at 21:30. It creates the billing csv file (detail, summary) for the delivery services in the delivery_service_topology.csv file, which has the billing item.

The path to view the billing.csv is:

Go to LWF node and navigate to */home/bnisplunk/data/billing*

Running billing manually

To run the billing manually, perform the following steps:

1. Login to the JS node and navigate to *opt/splunk/etc/apps/CDN_JS/bin*
2. In the above path, run *./hourlyDataCheck.sh -F YYYYMMDD* (replace the date for which hourlyDataCheck needs to be executed).

   The above mentioned script, marks the status as FIXED for every hour of that date in the "cdn_billing_session" index, which means there are NO missing logs.

   To verify this, perform the following steps:

   a) Login to JS node and navigate to /*opt/splunk/bin*

   b) Run *./splunk search 'index=cdn_billing_session | table Status,TimeId*.

   c) Enter the username and password; **Username**: admin and **Password**: Beaumaris1

   d) Check the status by verifying that the record is "FIXED YYYYMMDD". This implies that it is in FIXED status for all 24 hours in date YYYYMMDD.
3. In the path mentioned in step 1, run *./repeatCheck.sh -F YYYYMMDD* (replace the date for which repeatCheck needs to be executed).

   This will mark the status as FORCED for every hour of that date in the "cdn_billing_session" index. Also, an "INDEXED" record for that day is created. This implies that all the logs of that date are indexed. You can verify this by performing the following steps:

   a) Login to the JS node and navigate to */opt/splunk/bin*

   b) Run *./splunk search 'index=cdn_billing_session | table Status,TimeId'*

   c) Enter the username and password; **Username**: admin and **Password**: Beaumaris1

   d) Check the status by verifying that the record is "INDEXED YYYYMMDD. This implies that the date YYYYMMDD is already indexed.
4. Login to the LWF node and navigate to *opt/splunkforwarder/etc/apps/Billing/bin* and run *./billing.sh*. The billing files will be generated under the dir "/home/bnisplunk/data/billing".

   a) Login to the JS node and navigate to */opt/splunk/bin*

   b) Run *./splunk search 'index=cdn_billing_session | table Status,TimeId.*

   c) Enter the username and password; **Username**: admin and **Password**: Beaumaris1

   d) Check the status by verifying that the record is "BILLED YYYYMMDD". This implies that billing records have been generated for the date YYYYMMDD.

   The generated CSV files will have the following fields:

   Detailed csv

   Delivery_Service:<Delivery Service Name> FQDN:<fqdn> provider:<Provider Name> reseller:<Reseller Name> StartTime,EndTime,ClientIP,ServerIP,URL,MB_Bytes_Delivered,error_code

Summary csv
Date,Total_GB_Bytes_Delivered,Total_Session_Declined_due_to_quota_limits,Total_Sessions_Delivered

Reports

This feature allows you to view the daily, weekly, and monthly reports for CDN traffic, traffic summary by delivery servers, traffic summary by delivery services, delivery server traffic, and delivery service traffic.

To access this feature, from the main page, select **Analytics** > **Reports**.

Daily

To view the daily reports, select **Daily** from the Reports main page.

CDN Traffic [5 min Intervals]

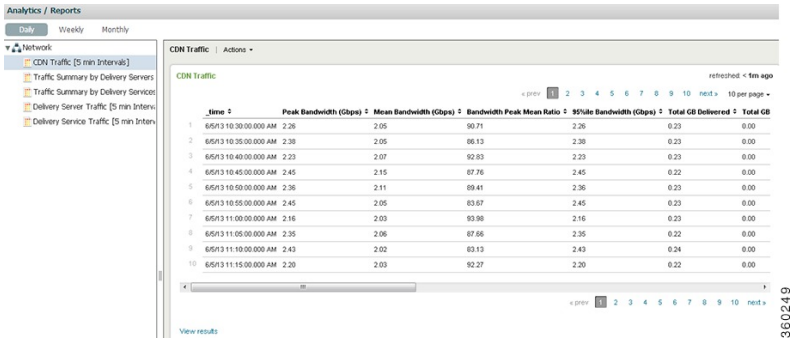


Table 52: CDN Traffic [5 min Intervals] Table & Description

Table	Description
CDN Traffic [5 min Intervals]	Illustrates CDN Traffic for the past day in 5 minute intervals.
Table Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Traffic Summary by Delivery Servers

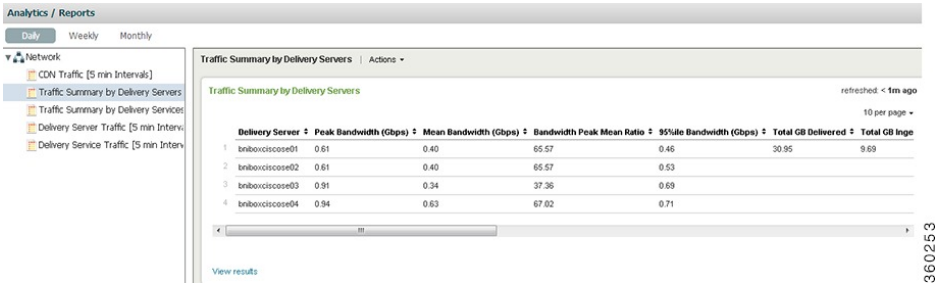


Table 53: Traffic Summary by Delivery Servers Table & Description

Table	Description
Traffic Summary by Delivery Servers	Illustrates the traffic summary for the past day for each delivery server.
Information	The information within this table is: delivery server, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Traffic Summary by Delivery Services

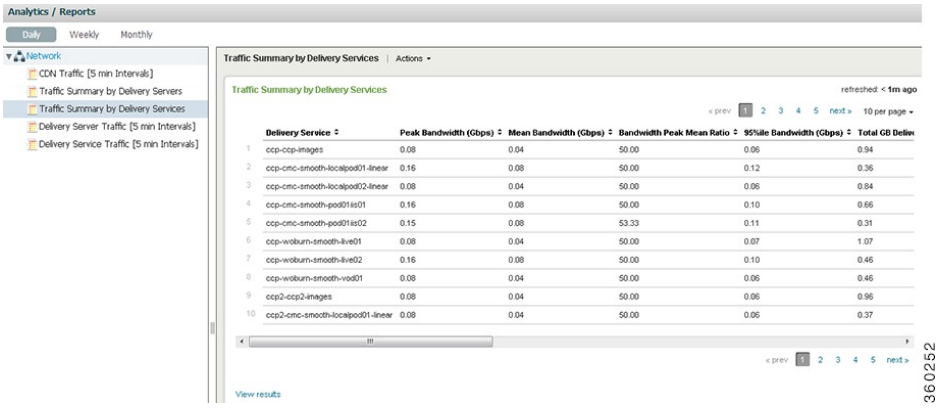


Table 54: Traffic Summary by Delivery Services Table & Description

Table	Description
Traffic Summary by Delivery Services	Illustrates the traffic summary for the past day for each delivery service.

Table	Description
Information	The information within this table is: delivery service, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Delivery Server Traffic [5 min Intervals]

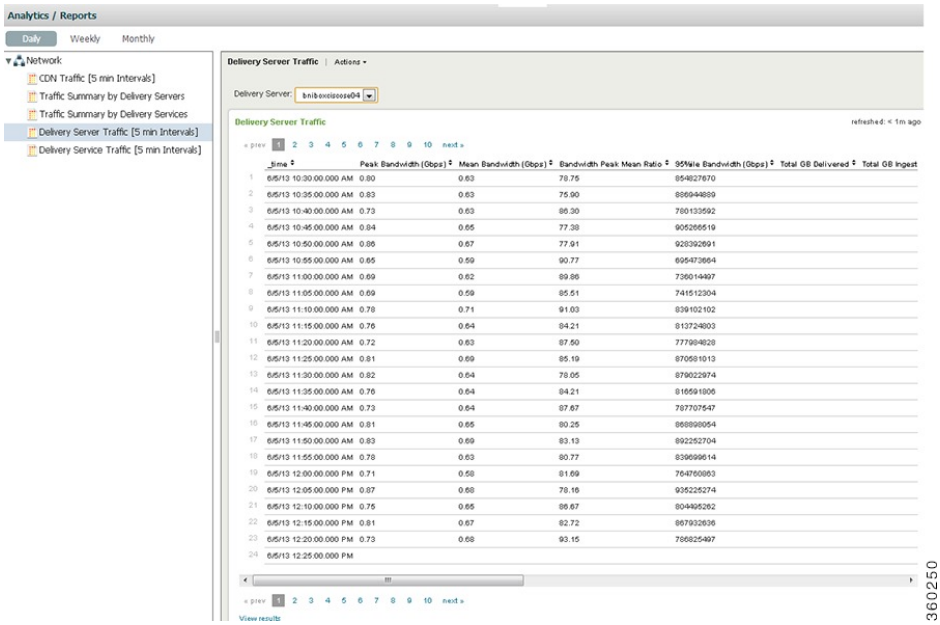


Table 55: Delivery Server Traffic [5 min Intervals] Table & Description

Table	Description
Delivery Server Traffic [5 min Intervals]	Illustrates the delivery server traffic details for a selected delivery server in 5 minute intervals
Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Choose the required delivery server from the **Delivery Server** drop-down list located above the chart.

Delivery Service Traffic [5 min Intervals]

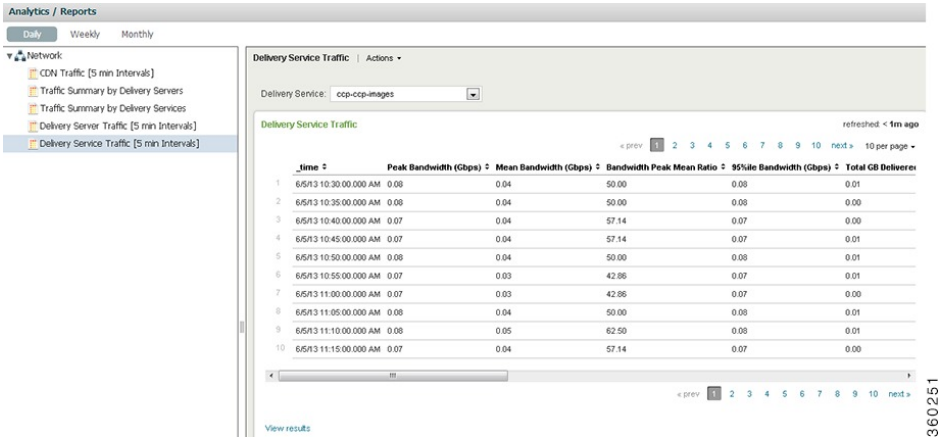


Table 56: Delivery Service Traffic [5 min Intervals] Table & Description

Table	Description
Delivery Service Traffic [5 min Intervals]	Illustrates the delivery service traffic details for a selected delivery service in 5 minute intervals.
Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Choose the required delivery service from the **Delivery Service** drop-down list located above the chart.

Weekly

To view the daily reports, select **Weekly** from the Reports main page.

CDN Traffic [1 hour Intervals]

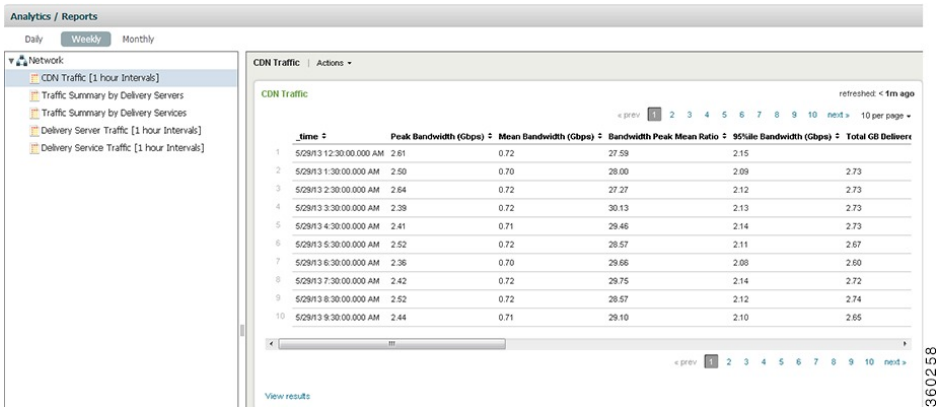


Table 57: CDN Traffic [1 hour Intervals] Table & Description

Table	Description
CDN Traffic [1 hour Intervals]	Illustrates CDN Traffic for the past week in 1 hour intervals.
Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Traffic Summary by Delivery Servers

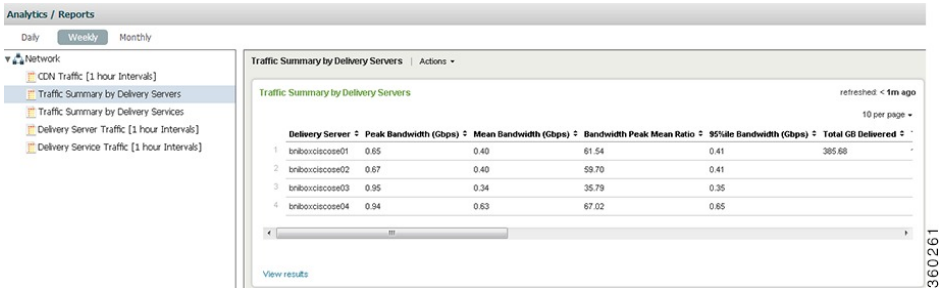


Table 58: Traffic Summary by Delivery Servers Table & Description

Table	Description
Traffic Summary by Delivery Servers	Illustrates the traffic summary for the past week for each delivery server.

Table	Description
Information	The information within this table is: delivery server, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Traffic Summary by Delivery Services

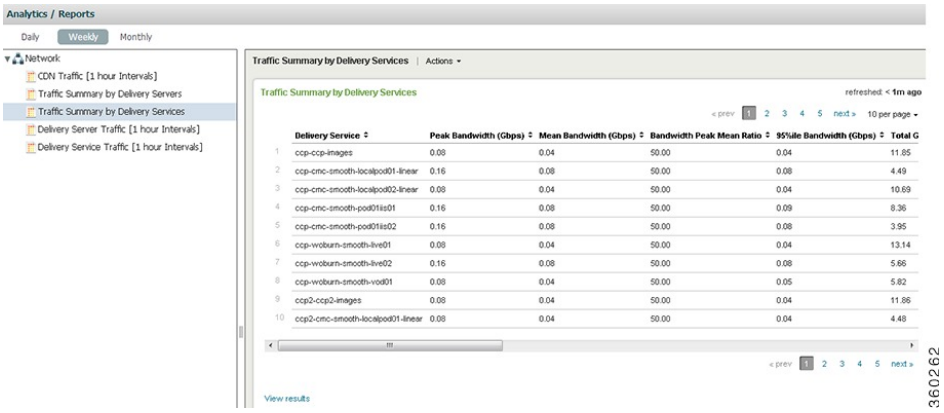


Table 59: Traffic Summary by Delivery Services Table & Description

Chart	Description
Traffic Summary by Delivery Services	Illustrates the traffic summary for the past week for each delivery service.
Information	The information within this table is: delivery service, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Delivery Server Traffic [1 hour Intervals]

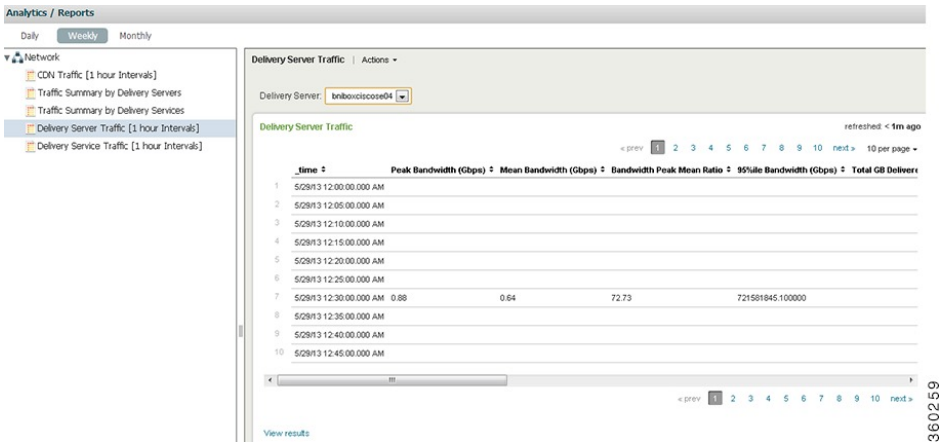


Table 60: Delivery Server Traffic [1 hour Intervals] Table & Description

Table	Description
Delivery Server Traffic [1 hour Intervals]	Illustrates the delivery server traffic details for a selected delivery server in 1 hour intervals
Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Choose the required delivery server from the **Delivery Server** drop-down list located above the chart.

Delivery Service Traffic [1 hour Intervals]

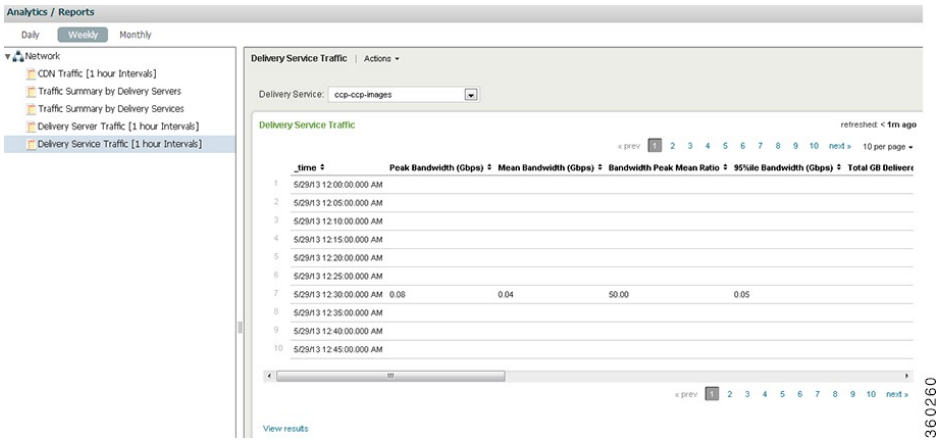


Table 61: Delivery Service Traffic [1 hour Intervals] Table & Description

Table	Description
Delivery Service Traffic [1 hour Intervals]	Illustrates the delivery service traffic details for a selected delivery service in 1 hour intervals.
Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Choose the required delivery service from the **Delivery Service** drop-down list located above the chart.

Monthly

To view the daily reports, select **Monthly** from the Reports main page.

CDN Traffic [1 day Intervals]

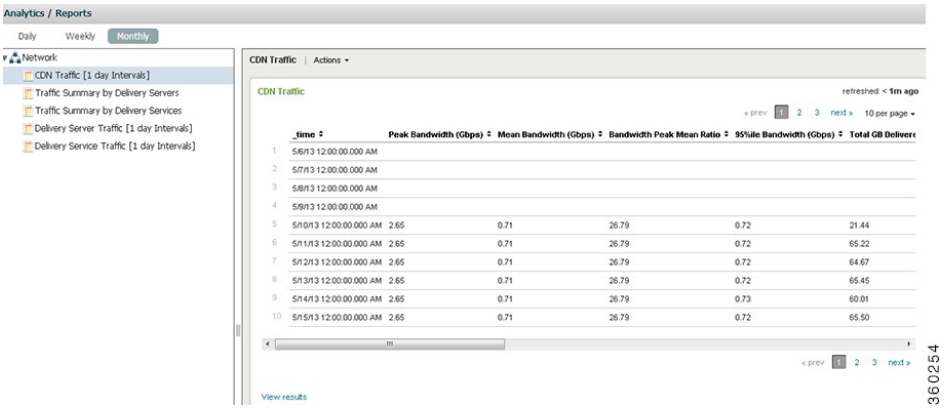


Table 62: CDN Traffic [1 day Intervals] Table & Description

Table	Description
CDN Traffic [1 hour Intervals]	Illustrates CDN Traffic for the past month in 1 day intervals.

Table	Description
Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Traffic Summary by Delivery Servers

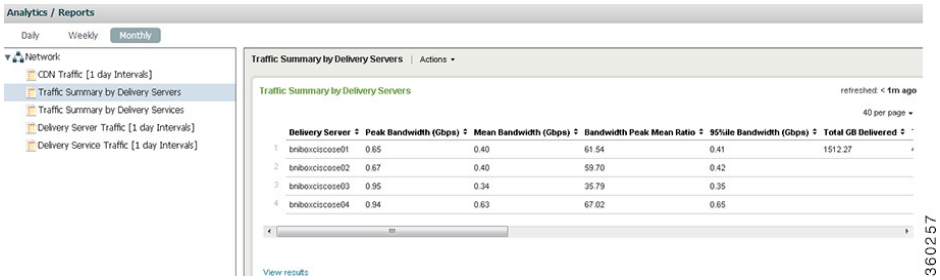


Table 63: Traffic Summary by Delivery Servers Table & Description

Table	Description
Traffic Summary by Delivery Servers	Illustrates the traffic summary for the past month for each delivery server.
Information	The information within this table is: delivery server, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Traffic Summary by Delivery Services

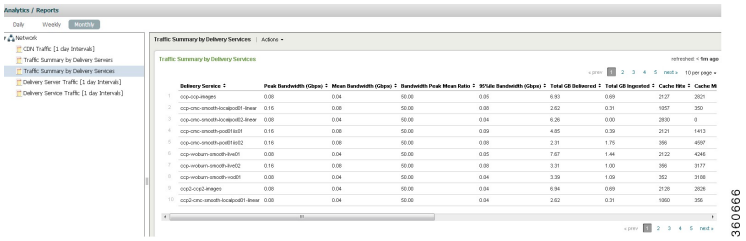


Table 64: Traffic Summary by Delivery Services Table & Description

Table	Description
Traffic Summary by Delivery Services	Illustrates the traffic summary for the past month for each delivery service.
Information	The information within this table is: delivery service, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Delivery Server Traffic [1 day Intervals]

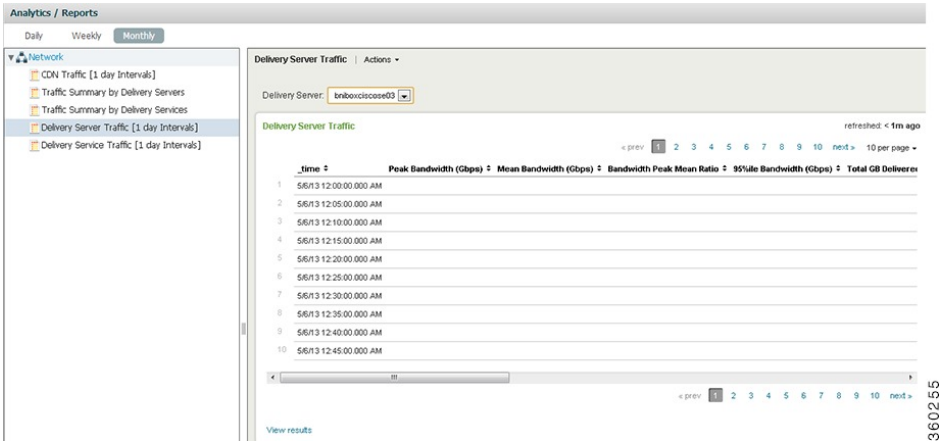


Table 65: Delivery Server Traffic [1 day Intervals] Table & Description

Table	Description
Delivery Server Traffic [1 hour Intervals]	Illustrates the delivery server traffic details for a selected delivery server in 1 day intervals
Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

Choose the required delivery server from the **Delivery Server** drop-down located above the chart.

Delivery Service Traffic [1 day Intervals]

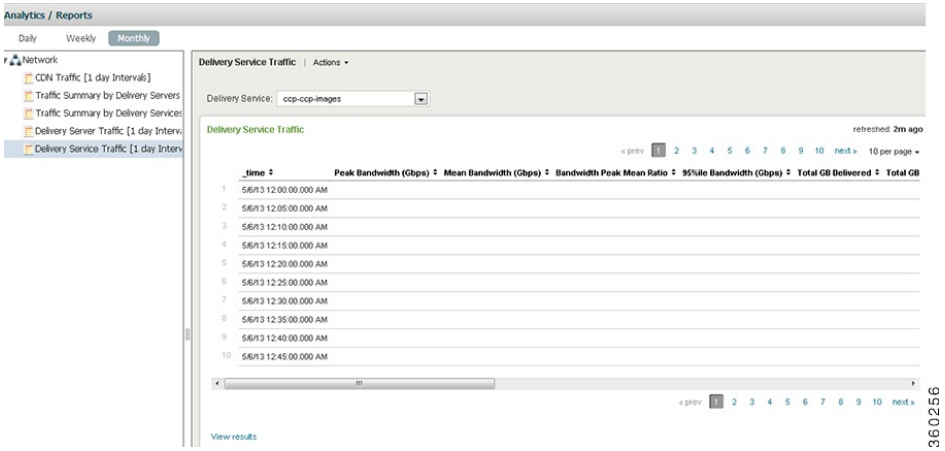


Table 66: Delivery Service Traffic [1 day Intervals] Table & Description

Table	Description
Delivery Service Traffic [1 hour Intervals]	Illustrates the delivery service traffic details for a selected delivery service in 1 day intervals.
Information	The information within this table is: _time, peak bandwidth, mean bandwidth, bandwidth peak mean ratio, 95%ile bandwidth, total GB delivered, total GB ingested, cache hits, cache misses, cache hit ratio, mean sessions, peak sessions, sessions peak mean ratio, 95%ile sessions, total requests, successful requests, unsuccessful requests, 4xx errors, 5xx errors, success %.

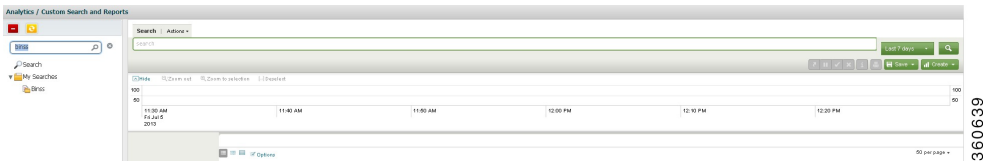
Choose the required delivery service from the **Delivery Service** drop-down list located above the chart.

Custom Searches and Reports

This feature displays all the saved searches and reports. The logged in user can view both, public and private searches. However, the logged in user cannot view the private searches saved by another user. In this feature, only the Delete and Refresh options are available. The user will not be able to modify any saved searches. To view Saved Searches, perform the following:

From the main page, select **Analytics** > **Custom Searches and Reports**.

Note When a user has multiple saved searches, enter the search name in the filter, which is located in the left pane and the particular saved search will be displayed.



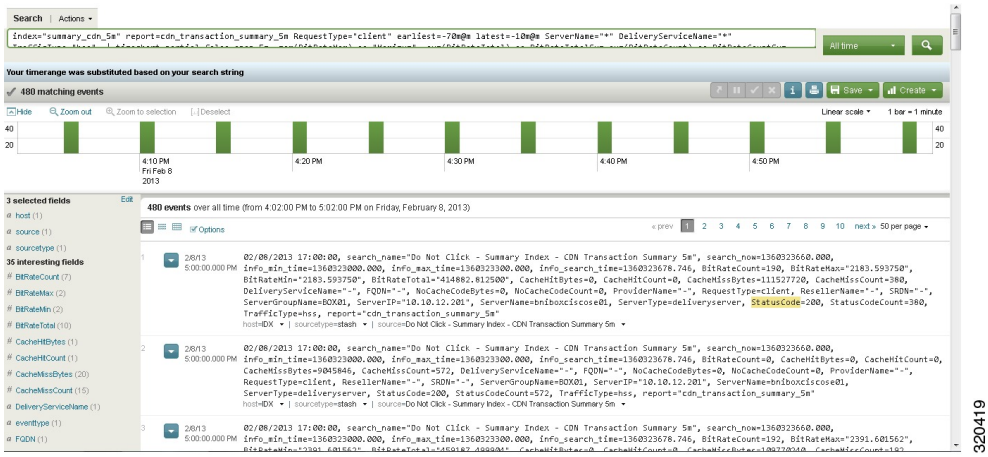
Saving a Search

You can use this option to search queries and save the result.

To save a search, perform the following steps:

Step 1 From the main page, select **Analytics** > **Custom Searches and Reports**.

Step 2 Enter the query in the Search field and click .



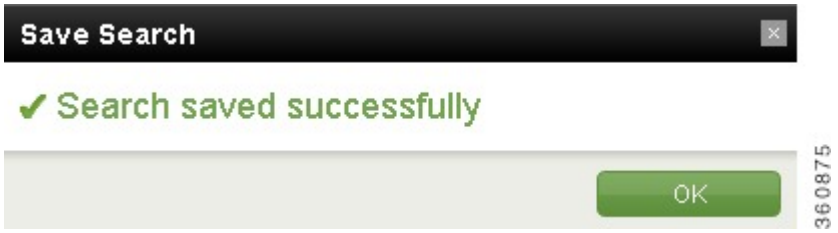
Step 3 From the **Save** drop-down list, select **Save search**...

Step 4 Enter the details in the Save Search dialog, as follows:

Table 67: Save Search Field & Description

Field	Description
Search name	Provide a name for your search. It can be a combination of alphabets and numbers.
Search string	This is automatically populated. The data populated will be the queried data.
Time range	Select the time period for which you want to gather data.
Share	• Enable the **Keep search private** button, if you do not want to display your search to other users. • Enable the **Share as read-only to all users of current app** button, if you wish to share your search with other users. **Note** The other users will have only the read-only permission.

Step 5 Click **Finish** and then click **OK** in the Search saved successfully dialog.



Deleting a Search

When a logged in user wants to delete a saved search, the application imposes the following restrictions:

Deleting the search saved by the logged in user

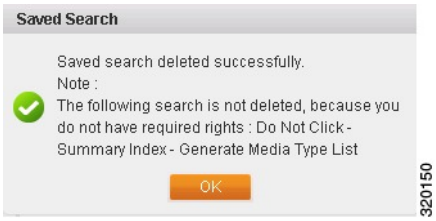
1. After navigating to Custom Searches and Reports, select the Search Name, which you want to delete and click .
2. Select **Yes** in the Confirmation dialog box.

Note Logged in users can delete only the searches saved by them.

Deleting multiple searches

1. After navigating to Custom Searches and Reports, select multiple Search Names that you wish to delete and click (to select multiple searches, hold down the **Shift** key and select the search names).
2. Select **Yes** in the Confirmation dialog box.

When you select multiple searches by selecting the searches saved by you and another user, the system will delete only the searches saved by you and the following error message is displayed.



Deleting saved searches of another user

When you delete a custom search saved by another user, the following error message is displayed.

Creating Custom Reports

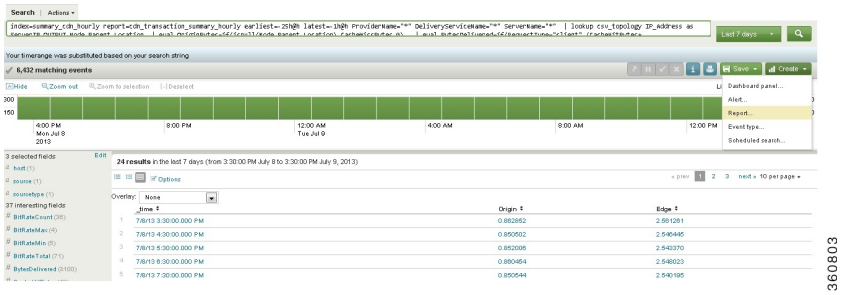
In this feature, you can create custom reports.

To create custom reports, perform the following steps:

Step 1 From the main page, click **Analytics** > **Custom Searches and Reports**.

Step 2 In the **Search** field, enter the query for which you want to generate a report and click .

Step 3 From the **Create** drop-down list, select **Report...**.



Step 4 In the CDN Analytics page, select the respective Report type and Fields.

Step 5 Click **Next Step** and enter the details.

Step 6 Click **Save**.

Step 7 In the Save Report dialog, enter all the details and click **Finish**.

Saving Custom Reports

In this feature, you can save the custom reports.

To save custom reports, perform the following steps:

Step 1 From the main page, click **Analytics** > **Custom Searches and Reports**.

Step 2 In the **Search** field, enter the query for which you want to save a report and click .

Step 3 From the **Save** drop-down list, select **Save report...**.

Step 4 Enter all the details in the Save Report dialog and click **Finish**.

Step 5 Click **OK** in the Save Report dialog.

To delete a report, click from the left pane.

Reporting Types

This section provides an overview of the reporting types (display format).

Following is a list of some of the available formatting options:

- Area
- Bar
- Column
- Line
- Pie
- Table

The available formatting options for each chart type are dependent on the fields and value types you choose to generate a report. For example, a report that is generated to display a count, has different formatting options than a report that is generated to display an average.

To define reports, use the drop-down lists and **X-** and **Y-axis** links to define the chart type and format. After you select your options, click **Apply** to generate the report output you defined.

Note Available **Formatting options** are dependent on the report type you select.

By default, reports are displayed in the column view. To change the view, define another report type.

In addition to viewing the whole report, you can view detailed data for a particular report segment by hovering that segment. The following example shows detailed report.

Area Chart Type

The area chart type is used to compare trends between two field values.

The area chart offers the following formatting options:

- X- and Y-axis formatting
- Stack mode
- Multi-series mode
- Legend placement
- Missing values

Column and Bar Chart Types

Column and bar chart types are used to generate a report that compares field values on the X- and Y- axis. The difference between a column and bar chart is the X- and Y- axis are reversed.

These charts offer the following formatting options:

- X- and Y- axis formatting
- Stack mode
- Multi-series mode
- Legend placement

Line Chart Type

Line chart is used to generate a report that shows trends.

The line chart offers the following formatting options:

- X- and Y-axis formatting
- Multi-series mode view
- Missing values
- Legend placement

Pie Chart Types

The pie chart is used to show proportional relationships between the data.

This chart type offers the following formatting options:

- Chart title
- X- and Y-axis formatting
- Legend placement

Table Reports

This section provides an overview of the **Table** report type.

You can sort each column by ascending and descending order, by toggling the arrows in each column.

Table 68: Table Report Filtering

Option	Description
Results per page	Specify how many lines of data you want to display
Overlay	Specify if you want to highlight certain data. Options are: • **None**: Do not highlight data • **Heat Map**: Produces a gradient color overlaid on a table of counts, where the highest values are highlighted in red, the lowest values are in white, and the values in-between are shaded in graduated colors from white to red. • **High and low values**: Highlight the highest and lowest values in the whole data set.

By default, summary information is displayed for each row of data.

To view detailed information, double-click the row for which you want detailed information. To return to the summary view, close the detailed window by clicking the **Close** (x) icon.

Custom Dashboards

This feature allows the CDN operators to create and save dashboards using the search application. You can view the list of all custom dashboards created by you and other users.

To access this feature, from the main page, select **Analytics** > **Custom Dashboards**. You can view the custom dashboards in the left pane. Click the arrow next to **My Dashboards** and select the custom dashboard, which you want to view. The details will be displayed in the right pane.

This feature allows you to create, delete, and refresh dashboards. By default, the dashboards are grouped by username.

Note All Splunk functionalities (related links/navigation) that are part of custom dashboards are out of scope.

Adding a Custom Dashboard

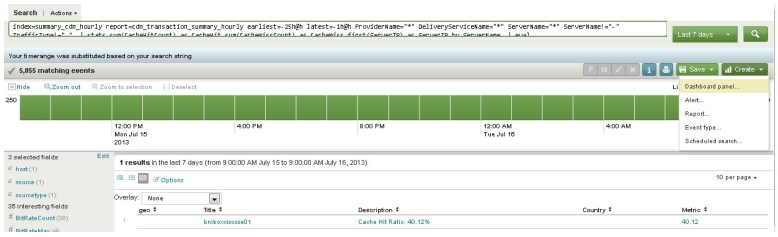
To add a custom dashboard, perform the following:

Step 1 Click **Analytics** > **Custom Dashboards**.

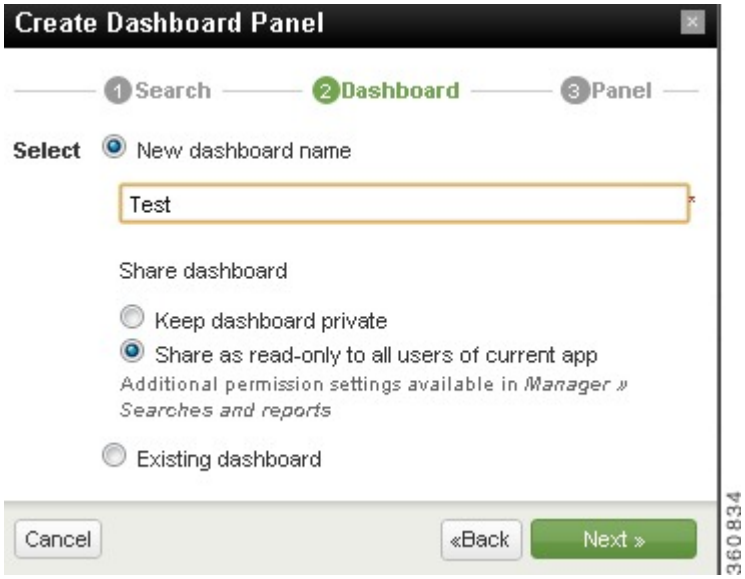
Step 2 Click  .

Step 3 On the right pane, enter the query in the Search field and click  .

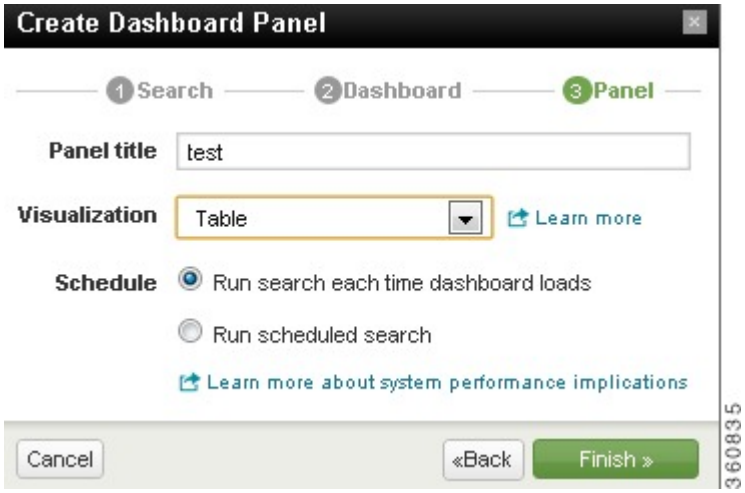
Step 4 Click the **Create** drop-down list and select **Dashboard panel...**.



Step 5 In the Create Dashboard Panel dialog, enter the Search name and Time range; click **Next**.



Step 6 In the New dashboard name field, provide a name for the dashboard and click **Next**.



If it is an existing dashboard, click the Existing dashboard radio button and click **Next**. From the **Choose...** drop-down list, select the dashboard. Also, choose whether you prefer to share the dashboard with other users or you prefer to keep it private.

Step 7 Provide the Panel title, choose from the Visualization drop-down list on how you want the dashboard to appear, and click the preferred **Schedule** radio button.

Step 8 Click **Finish** and then, **OK**.

Note The respective searches will be saved under Custom Searches and Reports.

Deleting a Custom Dashboard

To delete a custom dashboard, perform the following:

Step 1 Click **Analytics** > **Custom Dashboards**.

Step 2 From the left pane, select the custom dashboard, which you want to delete and click .

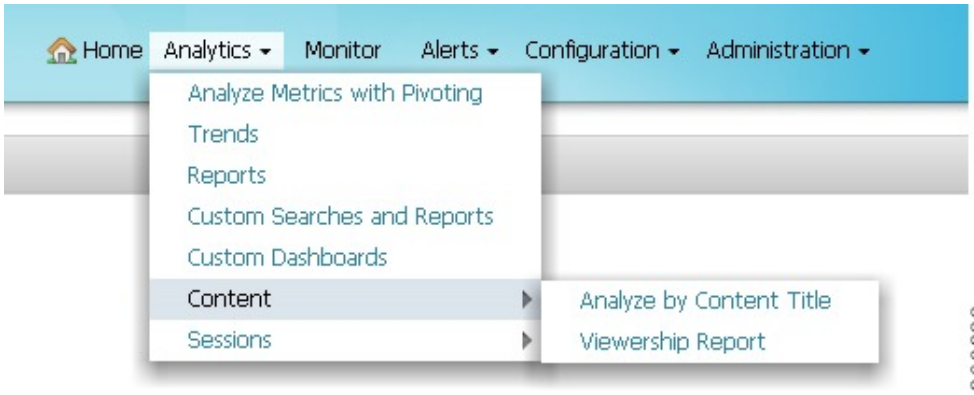
Step 3 Click **Yes** in the Confirmation dialog and then click **OK** in the Custom Dashboard dialog.

Note You can delete only the custom dashboard, which you have saved.

If you are deleting one or more searches that is being used by one or more custom dashboards, then those dashboards will not work. Also, the search saved as part of custom dashboards will have to be deleted manually.

Content

In this feature, the users will be able to analyze the data, based on the content title. They can also generate viewership report, based on various metrics.



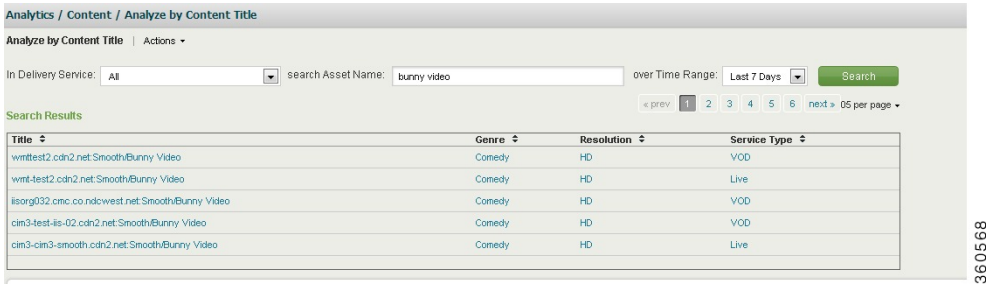
Analyze by Content Title

This feature provides a platform for the users to analyze individual asset (content title), based on various metrics such as Usage, Audience, QoS, and Errors.

Step 1 From the main page, select **Analytics** > **Content** > **Analyze by Content Title**.

Step 2 Choose the desired delivery service, select the time range from the respective drop-down lists, and enter the search asset name in the Search Asset name field. Then, click **Search**.

Note Entering certain search asset name values such as space and individual characters in the **Search Asset Name** text box will display large results. This may impact the system's performance.

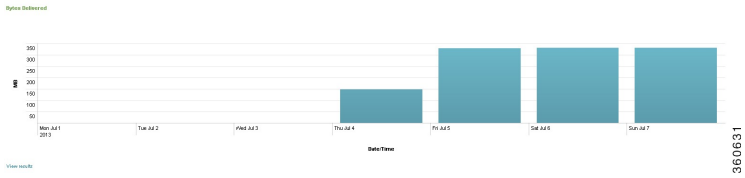


Step 3 From the list of unique content titles that are displayed in a tabular format, click the desired Title.
Different tabs such as Usage, Audience, QoS, and Errors for that particular title are displayed. Click the respective tabs to view the corresponding charts.

The different charts are explained in detail here.

Usage

Bytes Delivered



The following table describes the information in the chart:

Table 69: Bytes Delivered Chart & Description

Chart	Description
Bytes Delivered	Illustrates the bytes delivered (MB) over time for the given content title.

Chart	Description
Chart Information	The information within this chart is shown in a column graph with the Date/Time along the X-axis and the bytes delivered in MB along the Y-axis.
Formula	The formula used to derive this graph is: the total bytes delivered for the given content title plotted over time.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Bytes Delivered by City

This map illustrates the bytes delivered per city (MB) for the given content title.

Note The public IPs that are not resolved by MaxMind will be represented as '-' in the maps.

Bytes Delivered by City

The following table describes the information in the chart:

Table 70: Bytes Delivered by City Table & Description

Table	Description
Bytes Delivered by City	Illustrates the bytes delivered (MB) per city for the given content title.
Information	The information within this table are City and MB.

Table	Description
Formula	The formula used is: total bytes delivered for the given content title in each city.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Note The city will be resolved only for public IPs. IPs which cannot be resolved by MaxMind will not be displayed.

Bytes Delivered by ISP and Net Speed

The following table describes the information in the tabular column:

Table 71: Bytes Delivered by ISP and Net Speed Table & Description

Table	Description
Bytes Delivered by ISP and Net Speed	Illustrates the bytes delivered (MB), grouped by ISP or Net Speed for the given content title.
Table Information	The information within this table are ISP or Net Speed and MB.
Formula	The formula used is: total bytes delivered for the given content title grouped by the client ISP or Net Speed.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Note Other than public IPs, "unknown" value will be displayed.

Bytes Delivered by Client Type

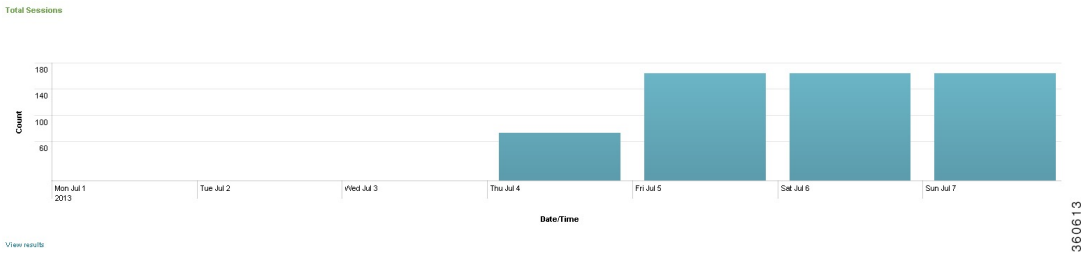
The following table describes the information in the tabular column:

Table 72: Bytes Delivered by Client Type Table & Description

Table	Description
Bytes Delivered by Client Type	Illustrates the bytes delivered per client type (MB) for the given content title.
Table Information	The information within this table are Client Type and MB.
Formula	The formula used is: total bytes delivered for the given content title grouped by the client type.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Audience

Total Sessions

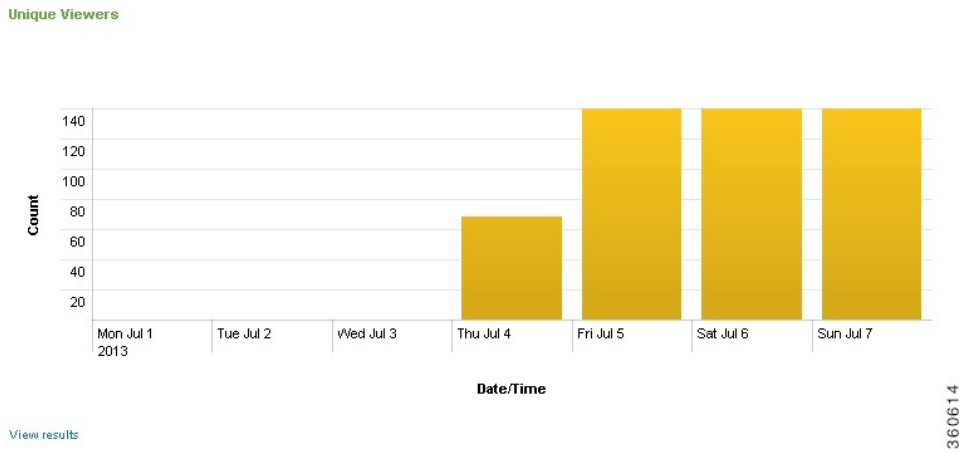


The following table describes the information in the chart:

Table 73: Total Sessions Chart & Description

Chart	Description
Total Sessions	Illustrates the number of sessions over time for the given content title.
Chart Information	The information within this chart is shown in a column graph with the Date/Time along the X-axis and the Total Sessions Count along the Y-axis.
Formula	The formula used to derive this graph is: the total number of sessions for a given content title plotted over time.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Unique Viewers



The following table describes the information in the chart:

Table 74: Unique Viewers Chart & Description

Chart	Description
Unique Viewers	Illustrates the number of unique viewers over time for the given content title.
Chart Information	The information within this chart is shown in a column graph with the Date/Time along the X-axis and the Unique Viewers count along the Y-axis.
Formula	The formula used to derive this graph is: the number of unique viewers for the given content title plotted over time.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Viewers by Download Size and Session Duration

The following table describes the information in the tabular column:

Table 75: Viewers by Download Size and Session Duration Table & Description

Table	Description
Viewers by Download Size and Session Duration	Illustrates the number of sessions grouped by download size or duration for the given content title.

Table	Description
Table Information	The information within this table are Download Size, Session Duration, and Count.
Formula	The formula used for Download Size is: the number of viewers bucketed by the download size in MB, for the given content title. The formula used for Duration is: the number of viewers bucketed by the average session duration for the given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Viewers by ISP and Net Speed

The following table describes the information in the tabular column:

Table 76: Viewers by ISP and Net Speed Table & Description

Table	Description
Viewers by ISP and Net Speed	Illustrates the number of sessions grouped by ISP and Net Speed for the given content title.
Table Information	The information within this table are ISP, Net Speed and the Viewer count.
Formula	The formula used to derive this graph is: the number of viewers grouped by client ISP/Net Speed for the given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Note Other than public IPs, "unknown" value will be displayed.

Viewers by City

The following table describes the information in the tabular column:

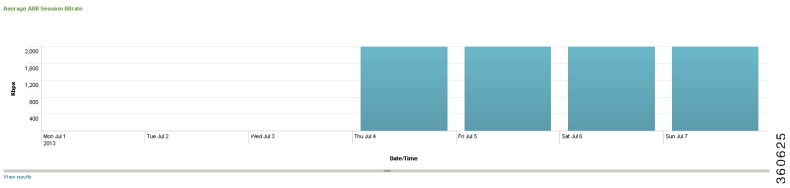
Table 77: Viewers by City Table & Description

Table	Description
Viewers by City	Illustrates the number of viewers per city for the given content title.
Table Information	The information within this table are City and Count.
Formula	The formula used to derive this graph is: the number of viewers in each city for the given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Note The city will be resolved only for public IPs. IPs which cannot be resolved by MaxMind will not be displayed.

QoS

Average ABR Session Bitrate



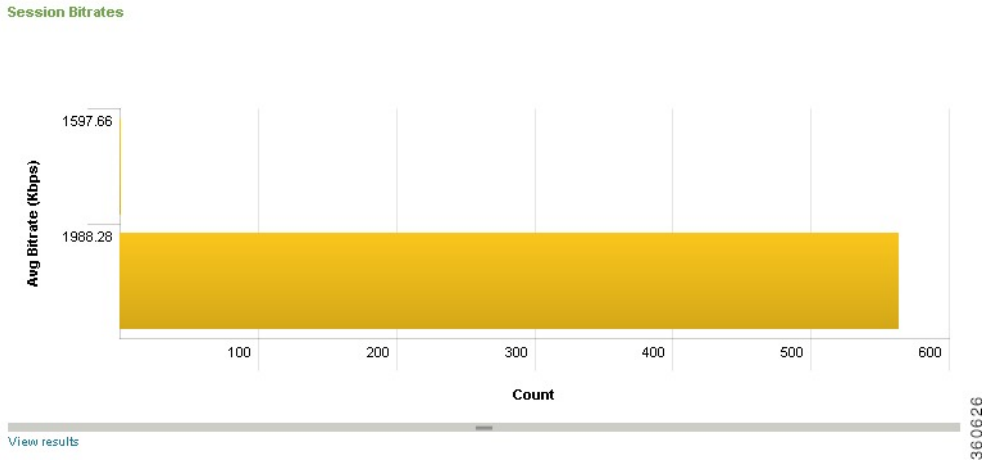
The following table describes the information in the chart:

Table 78: Average ABR Session Bitrate Chart & Description

Chart	Description
Average ABR Session Bitrate	Illustrates the average ABR session bitrate (Kbps) over time for the given content title.
Chart Information	The information within this chart is shown in a column graph with the Date/Time along the X-axis and the ABR Session Bitrate (Kbps) along the Y-axis.
Formula	The formula used to derive this graph is: the average bitrate plotted over time for the given content title.

Chart	Description
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Session Bitrates



The following table describes the information in the chart:

Table 79: Session Bitrates Chart & Description

Chart	Description
Session Bitrates	Illustrates the average bitrate over session count for the given content title.
Chart Information	The information within this chart is shown in a column graph with the Session Bitrate count along the X-axis and Avg Bitrate (Kbps) along the Y-axis.
Formula	The formula used to derive this graph is: the count of each bitrate for a given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

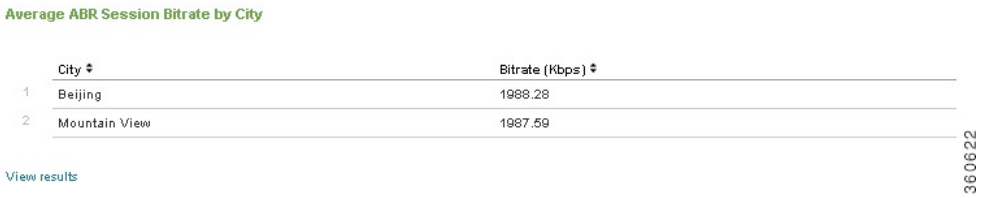
Average ABR Session Bitrate by Client Type

The following table describes the information in the table:

Table 80: Average ABR Session Bitrate by Client Type Table & Description

Table	Description
Average ABR Session Bitrate by Client Type	Illustrates the average ABR session bitrate (Kbps) per client type for the given content title.
Table Information	The information within this table are Client Type and Bitrate.
Formula	The formula used to derive this graph is: average ABR session bitrate (Kbps) for the given content title, grouped by the client type.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Average ABR Session Bitrate by City



The following table describes the information in the table:

Table 81: Average ABR Session Bitrate by City Table & Description

Table	Description
Average ABR Session Bitrate by City	Illustrates the average ABR session bitrate (Kbps) per city for the given content title.
Table Information	The information within this table are City and Bitrate.
Formula	The formula used to derive this graph is: average ABR session bitrate (Kbps) for the given content title in each city.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Note The city will be resolved only for public IPs. IPs which cannot be resolved by MaxMind will not be displayed.

Average ABR Session Bitrate by ISP and Net Speed

The following table describes the information in the table:

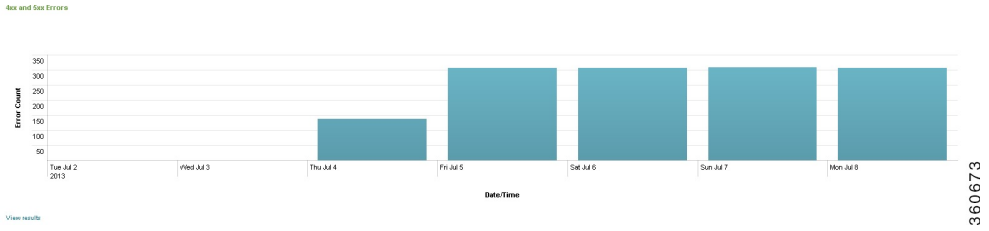
Table 82: Average ABR Session Bitrate by ISP and Net Speed Table & Description

Table	Description
Average ABR Session Bitrate by ISP and Net Speed	Illustrates the average ABR session bitrate (Kbps) grouped by ISP and Net Speed for the given content title.
Table Information	The information within this table are Client ISP/Net Speed and Bitrate.
Formula	The formula used to derive this graph is: average ABR session bitrate (Kbps) for the given content title grouped by the client ISP and Net Speed.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Note Other than public IPs, "unknown" value will be displayed.

Errors

4xx and 5xx Errors



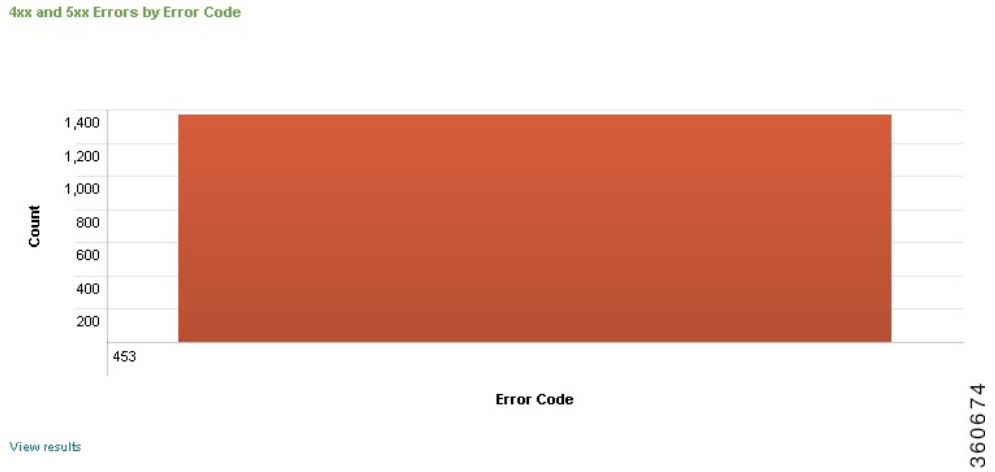
The following table describes the information in the chart:

Table 83: 4xx and 5xx Errors Chart & Description

Chart	Description
4xx and 5xx Errors	Illustrates the number of 4xx and 5xx (client and server) errors over time for the given content title.

Chart	Description
Chart Information	The information within this chart is shown in a column graph with the Date/Time along the X-axis and the Error count along the Y-axis.
Formula	The formula used to derive this graph is: the number of 4xx and 5xx errors plotted over time for the given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

4xx and 5xx Errors by Error Code

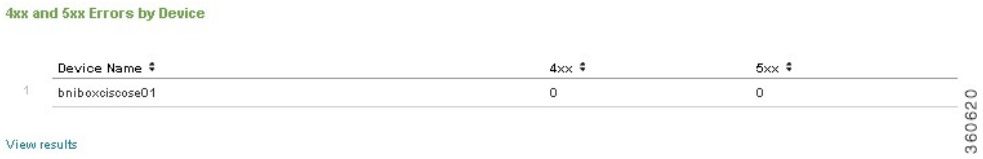


The following table describes the information in the chart:

Table 84: 4xx and 5xx Errors by Error Code Chart & Description

Chart	Description
4xx and 5xx Errors by Error Code	Illustrates the number of 4xx and 5xx (client and server) errors grouped by error codes for the given content title.
Chart Information	The information within this chart is shown in a column graph with the Error Code along the X-axis and the Error count along the Y-axis.
Formula	The formula used to derive this graph is: the number of 4xx and 5xx errors grouped by the respective error codes for the given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

4xx and 5xx Errors by Device

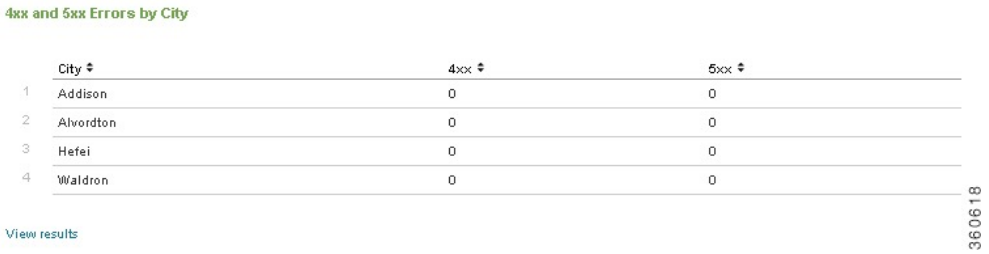


The following table describes the information in the table:

Table 85: 4xx and 5xx Errors by Device Table & Description

Table	Description
4xx and 5xx Errors by Device	Illustrates the number of 4xx and 5xx (client and server) errors per device (delivery servers and service routers) for the given content title.
Table Information	The information within this table are Device Name, 4xx, and 5xx Errors.
Formula	The formula used to derive this graph is: the number of 4xx and 5xx errors occurring in each device (delivery servers and service routers) for the given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

4xx and 5xx Errors by City



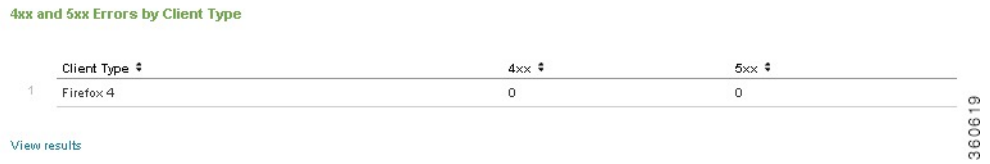
The following table describes the information in the table:

Table 86: 4xx and 5xx Errors by City Table & Description

Table	Description
4xx and 5xx Errors by City	Illustrates the number of 4xx and 5xx (client and server) errors per city for the given content title.
Table Information	The information within this table are City, 4xx, and 5xx errors.

Table	Description
Formula	The formula used to derive this graph is: the number of 4xx and 5xx errors occurring in each city for the given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

4xx and 5xx Errors by Client Type



The following table describes the information in the table:

Table 87: 4xx and 5xx Errors by Client Type Table & Description

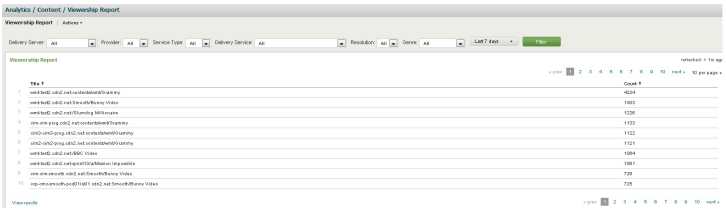
Table	Description
4xx and 5xx Errors by Client Type	Illustrates the number of 4xx and 5xx (client and server) errors grouped by client type for the given content title.
Table Information	The information within this table are Client Type, 4xx, and 5xx errors.
Formula	The formula used to derive this graph is: the number of 4xx and 5xx errors occurring in each client type for the given content title.
Filters	This chart uses Delivery Service, and Time Range (Previous day and Last 7 days), as filters.

Viewership Report

This feature provides a platform for the users to generate viewership reports, based on various metrics such as Delivery Server, Provider, Service Type, Delivery Service, Resolution, and Genre.

Step 1 From the main page, select **Analytics** > **Content** > **Viewership Report**.

Step 2 Select the Delivery Server, Provider, Service Type, Delivery Service, Resolution, and Genre from the respective drop-down lists and click **Filter**.
The viewership report is displayed.



Sessions

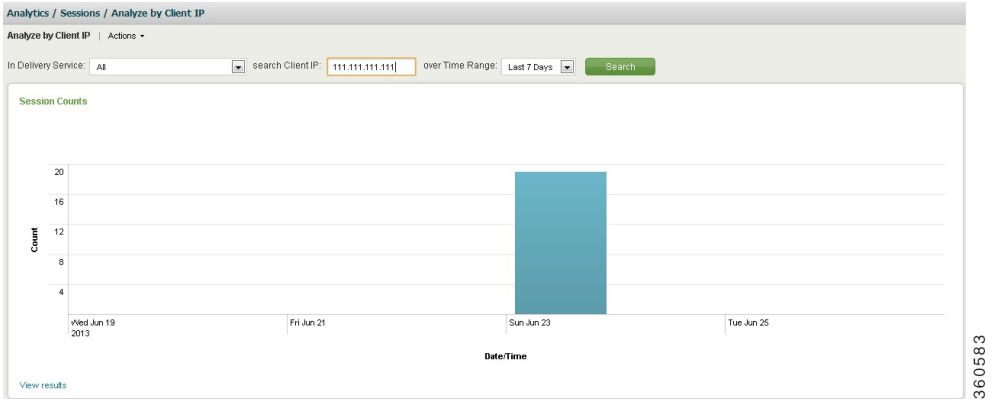
This feature provides a platform for users to analyze the individual client IP, based on various parameters such as sessions created for the IP, session duration, protocol used to serve the content, and title viewed during the session.

To access this feature, perform the following steps:

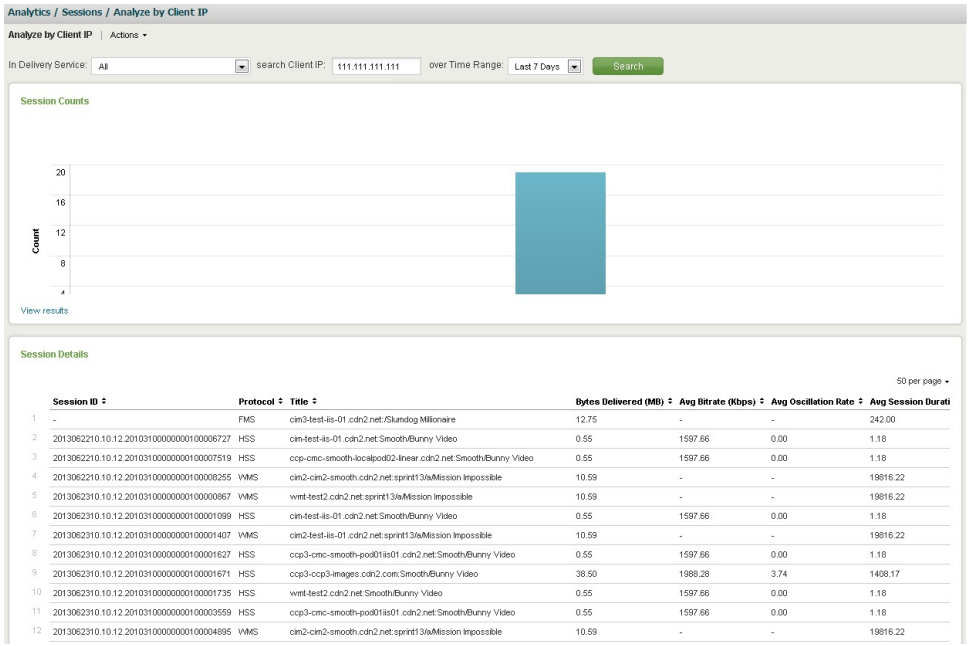
Step 1 From the main page, select **Analytics** > **Sessions** > **Analyze by Client IP**.

Step 2 Choose the desired delivery service, select the time range from the respective drop-down lists, and enter the client IP in the search Client IP field. Click **Search**.

Note In the search Client IP field, enter the exact client IP.



Step 3 From the sessions counts chart that is displayed, click the desired column. The session details will be displayed below the session count chart.



North Bound Application Programming Interface

North Bound Application Programming Interface (NB API) is a programming interface for north bound analytics systems to integrate with VDS-SM and leverage the data maintained in VDS-SM for higher level aggregation and analysis. VDS-SM provides a RESTful Web Services API to query data from VDS-SM for analytics. VDS-SM supports predefined queries/searches to query data corresponding to reports. Each predefined query/search is identified by a name, which corresponds to a particular dashboard. You can query the data by specifying the search name alone.

For example, in the CDN Traffic report, the search name is cdntraffic_daily.

To obtain the result for a query, you need to perform the HTTPS GET request using the following URL:

With Delivery Service Name

```
https://< UI
Node IP >:8443/bnimgmt/api/analytics/search/systemdefined/< searchname >?delsvc=<delivery
service name>
```

With Delivery Server Name

```
https://< UI
Node IP >:8443/bnimgmt/api/analytics/search/systemdefined/< searchname >?host=<delivery
server name>
```

Without Delivery Service or Delivery Server Name

```
https://< UI Node IP >:8443/bnimgmt/api/analytics/search/systemdefined/<searchName>
```

For example, to execute the search “cdntraffic_daily”, you need to perform GET request using the following URL:

```
https://<UI Node IP>:8443/bnimgmt/api/analytics/search/systemdefined/
cdntraffic_daily
```

You need to specify the Username and Password (CDN Operator Admin and CDN Viewer) for authentication in the “Authorization” header fields of the HTTPS GET request. For example, in command line tools such as curl, provide the following command with credentials:

```
curl -k -u bniadmin:admin --request GET 'https:// <UI Node IP
>:8443/bnimgmt/api/analytics/search/
systemdefined/cdntraffic_daily
```

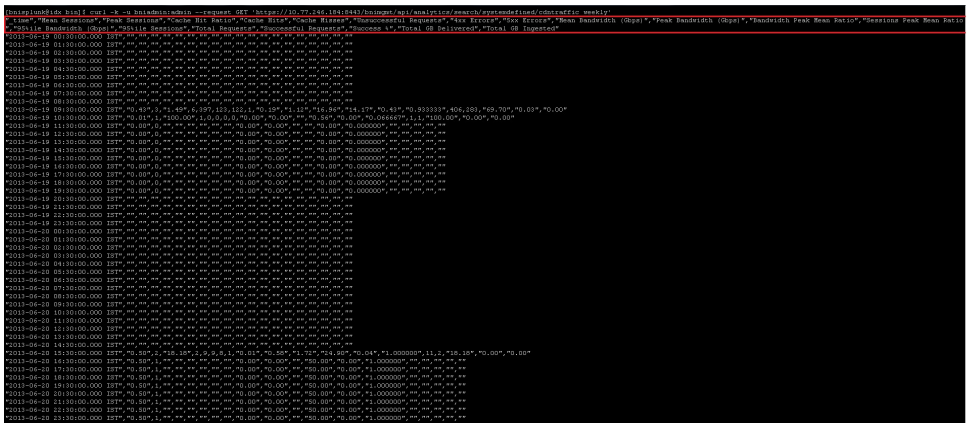
In the URL, you need to pass the delivery service name or delivery server name for a search and not any special characters or space.

Note The URL should be exactly the same as mentioned here and they should be entered in a single line. Also, HTTPS is authenticated through self-signed OpenSSL certificate for NB API and NB API does not support HTTP.

Result Format

Analytics API provides the results in CSV format. The first line is the header line with fields, followed by the data. Following is an example of Console Output.

curl -k -u bniadmin:admin --request GET
'https://10.77.246.184:8443/bnimgmt/api/analytics/search/systemdefined/cdntraffic_weekly'

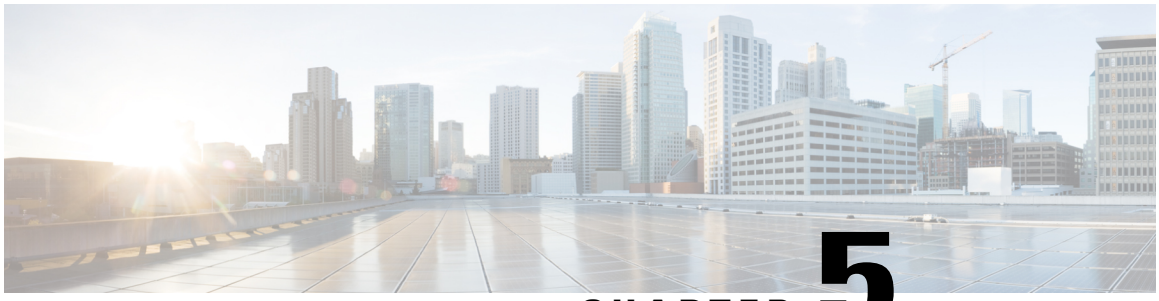


Supported Predefined Searches

Table 88: Search Name & Optional Parameters

Sl. No.	Search Name	Optional Parameters
1	cdntraffic_daily	
2	cdntraffic_weekly	
3	cdntraffic_monthly	
4	trafficsummary_by_deliveryservers_daily	
5	trafficsummary_by_deliveryservers_weekly	
6	trafficsummary_by_deliveryservers_monthly	

Sl. No.	Search Name	Optional Parameters
7	trafficsummary_by_deliveryservices_daily	
8	trafficsummary_by_deliveryservices_weekly	
9	trafficsummary_by_deliveryservices_monthly	
10	deliveryserver_traffic_daily	delivery_server_name
11	deliveryserver_traffic_weekly	delivery_server_name
12	deliveryserver_traffic_monthly	delivery_server_name
13	deliveryservice_traffic_daily	delivery_service_name
14	deliveryservice_traffic_weekly	delivery_service_name
15	deliveryservice_traffic_monthly	delivery_service_name



CHAPTER 5

Monitor

Monitor Overview

CDN hosts different content, such as live and archived, to viewers around the world. For the CDN Operators to quickly check the performance of the network, real-time monitoring is performed on Throughput, Cache Hit Ratio, Concurrent Active Sessions, and Responses.

Note Only Throughput, Cache Hit Ratio, Concurrent Active Sessions, and Responses charts are refreshed real-time (with minimum delay).

To access this feature, click **Monitor** from the main page.

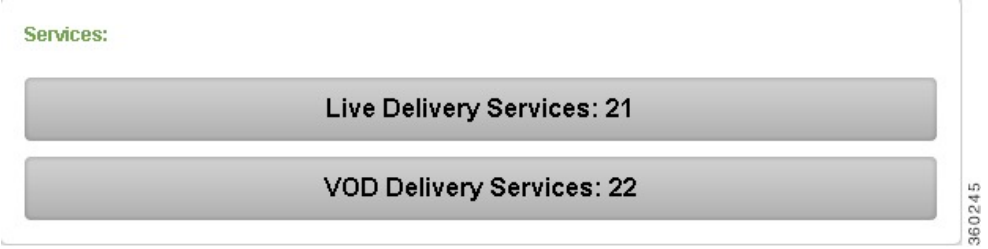
The following categories are displayed in Monitor:

- Services
- Network
- Throughput
- Cache Hit Ratio
- Concurrent Active Sessions
- Responses

These categories are explained in detail here.

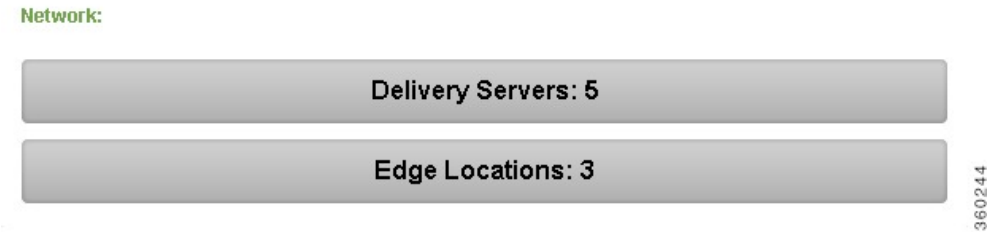
Services

Displays the number of live delivery services, and VOD delivery services. These values are refreshed every eight minutes.

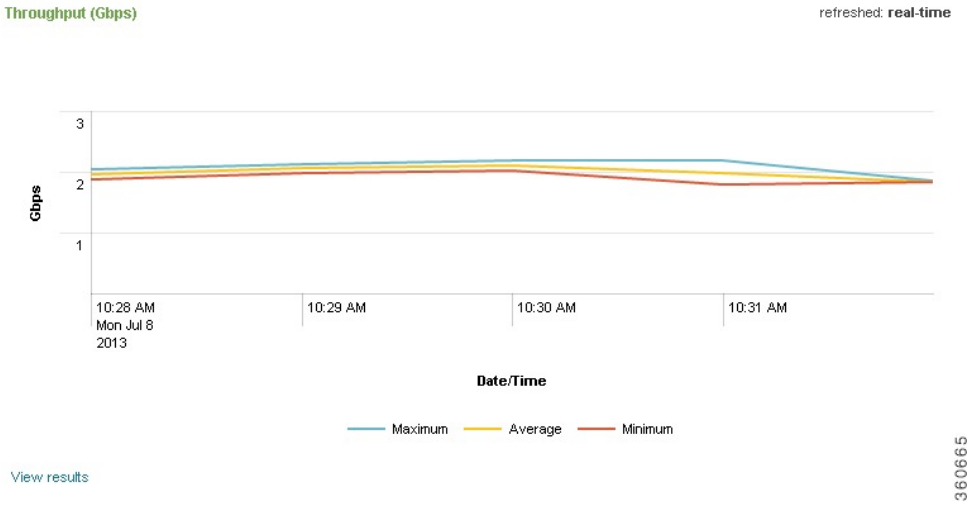


Network

Displays the number of delivery servers and edge locations. These values are refreshed every eight minutes.



Throughput (Gbps)



The following table describes the Throughput chart:

Table 89: Throughput Chart & Description

Chart	Description
Throughput	Illustrates the data delivered by the network at real-time.
Chart Information	The information within this chart is shown in a line graph with Date/Time along the X-axis and the throughput in Gbps along the Y-axis. The legends representing the graph are maximum, minimum, and average.

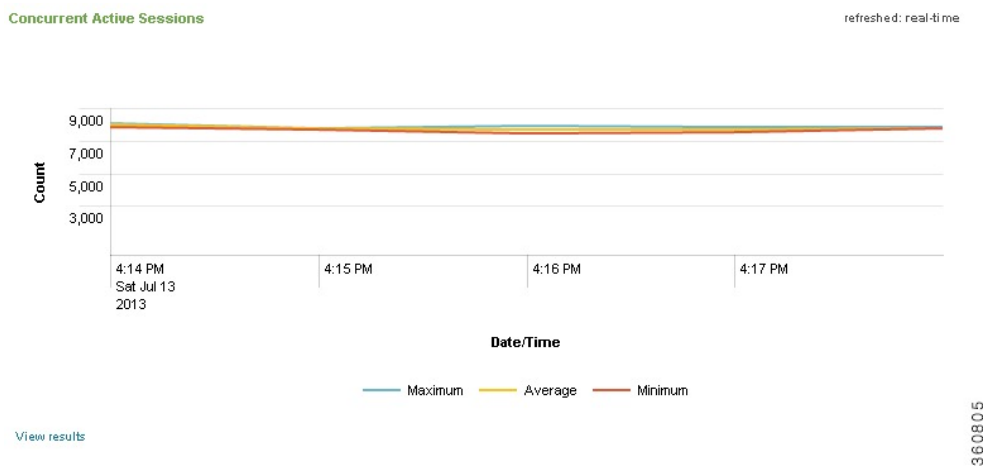
Cache Hit Ratio

The following table describes the Cache Hit Ratio chart:

Table 90: Cache Hit Ratio Chart & Description

Chart	Description
Cache Hit Ratio	Provides client request cache hit and miss percentage at real-time.
Chart Information	The information within this chart is shown in a stacked area graph with Date/Time along the X-axis and the cache hit/miss percentage in the Y-axis. The legends representing the graph are Cache Hit and Cache Miss.

Concurrent Active Sessions

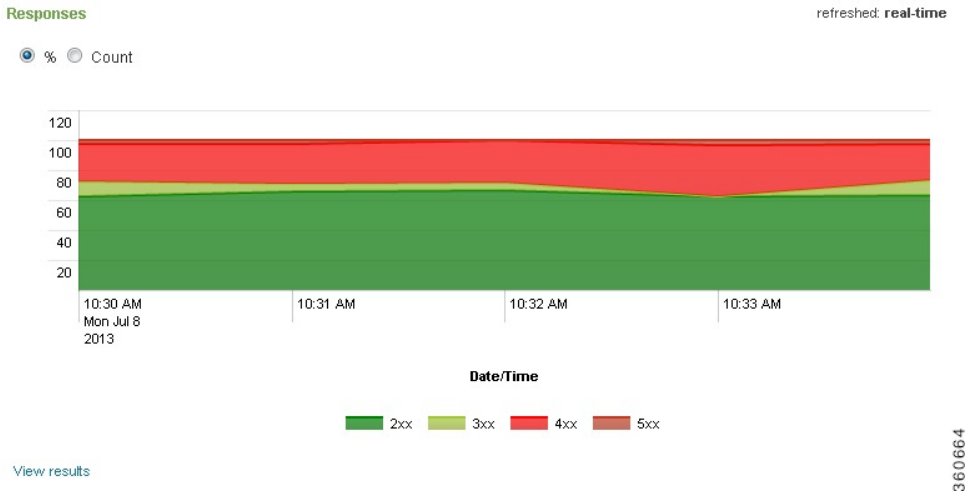


The following table describes the Concurrent Active Sessions chart:

Table 91: Concurrent Active Sessions Chart & Description

Chart	Description
Concurrent Active Sessions	Illustrates the concurrent client sessions at real-time.
Chart Information	The information within this chart is a line graph with Date/Time along the X-axis and Maximum, Minimum and Average count along the Y-axis. The legends representing the graph are maximum, average, and minimum.

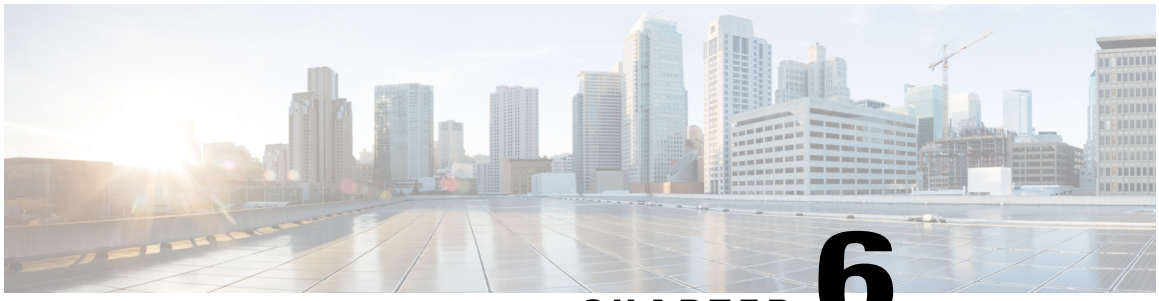
Responses



The following table describes the Responses chart:

Table 92: Responses Chart & Description

Chart	Description
Responses	Provides response codes count or percentage at real-time.
Chart Information	The information within this chart is shown in stacked area with Date/Time along the X-axis with the response count or percentage along the Y-axis. The legends representing the graph are 2xx, 3xx, 4xx, and 5xx.



CHAPTER 6

Alerts

Alerts Overview

Alert displays a count of events that are generated by the system.

Manage Alerts

The Alert Manager, which is accessed from the Alerts function, allows you to view the recently triggered alerts. It displays records of triggered alerts.

Following is a list of alerts:

- Application available–A service named in an alert has become available, meaning it has been recognized as in service by the system.
- Application unavailable–A service named in an alert became unavailable, meaning it is no longer visible on the network or is out of service.
- Delivery Service conflict–An alert is created when there is a conflict in the Device Service
- Device In Service–A topology device has transitioned to in service and is eligible to service requests, if it is operational.
- Device Out of Service–A topology device has transitioned to out of service and is not eligible to service requests, if it is operational.

Note Access the Alerts function by clicking **Alerts** from top-right of the main page.

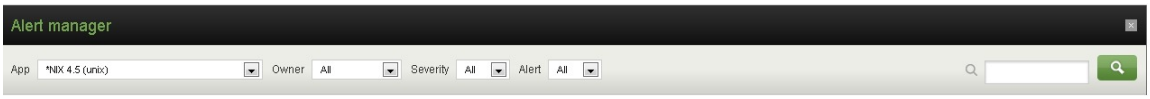
Using the Splunk web interface, you can configure the following:

- Create an alert

- Set up alert actions
- Set alert expirations
- Edit existing searches and alerts

Using the Alert Manager

From the main page, click **Alerts** > **Manage Alerts**.

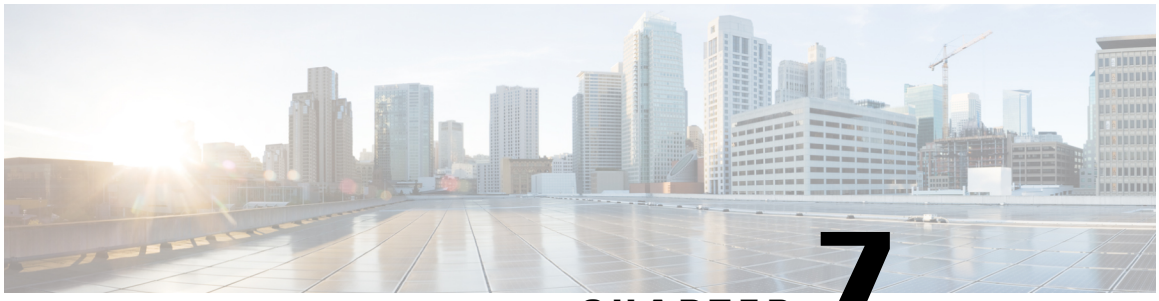


Here, you can perform the following:

- Filter the listings by application, owner, alert severity, and alert type.
- Search for keywords using the search box, which displays in the top-right corner of the Alert Manager window. The keyword search applies to fired alert names (which are the same as the names of the searches or reports upon which the alerts are based) and the alert severity (so you can search specifically for *Critical* severity alerts, if necessary).
- Manually delete individual alert records.

The Alert Manager window provides the following viewing options:

- **App**: Conductor VBO has three specific App alert types:
  - DBAnalytics (DBAnalytics): Analysis of MySQL database operations
  - VBO Session Analytics (SessionAnalytics): Displays thresholding for error counts and bandwidth usage
  - *NIX 4.5 (unix): Displays the health of the nodes (CPU, memory, disk space)
- **Owner**: Displays user login name
- **Severity**: Displays alerts by severity level, including those alert records that have been given a higher severity level, such as **High** or **Critical**
- **Alert**: Displays all alerts



CHAPTER 7

Configuration

VDS Manager Configuration

VDS Manager enables CDN Operators to deploy and manage the VDS-IS configuration such as delivery services.

Multi-Tiered and Multi-Tenancy

The Operator can manage the simple profile (name, contact info, and quota), users for content providers (CP) and Resellers. Once a CP or Reseller user is created, the newly created user can log in and view its own dashboards. The VDS Operator can manage the hierarchical relationship among CDN, CP, and Services. The CP or Reseller user can view dashboards at the Delivery Service level for all Delivery Services under its domain.

Services (1-to-1 with Delivery Service) are synchronized from the Content Delivery Service Manager (CDSM) periodically. All Delivery Services should be synchronized from the CDSM to the VDS Manager, including both live and VOD Content Delivery Services.

Adding a CDN

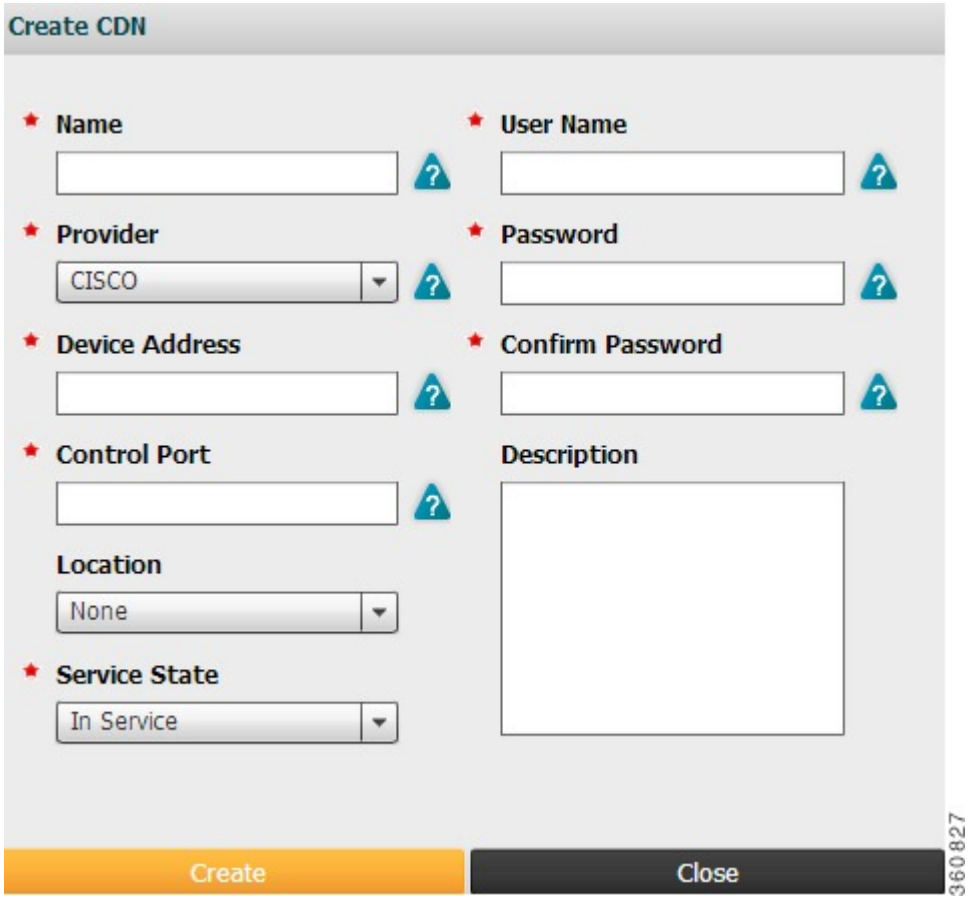
To deploy the VDS Service Manager, you must configure CDN. CDN enables the VDS Service Manager to gather topology information from the Service and allows the service to be controlled by the VDS Service Manager solution.

To add a CDN, perform the following steps:

Step 1 Login to the CDN Manager user interface.

Step 2 Select **Configuration** > **CDN**.
The CDN page, listing all configured CDN devices and their status is displayed.

Step 3 Click to create a new CDN.



In the Create CDN popup, enter the appropriate CDN information for the VDS-IS CDSM as mentioned here.

Table 93: Create CDN Field & Description

Field	Description
Name	A unique name for the device.

Field	Description
Provider	The content provider for this CDN.
Device Address	The IP address or Fully Qualified Domain Name (FQDN) of this device.
Control Port	A pre-existing port number specified for this device. Contact your System Administrator for this information.
Location	The location to which this device is associated.
Service State	The service state of the service: • In Service: Enables the service When a device is in this state, all read and write operations to this device are allowed. • Out of Service: Disables the service When a device is in this state, all write operations are not allowed. However, the read operation is still allowed, whereby the periodic sync, operational state check, and manual sync will still happen.
Username	The user name associated with the device.
Password/Confirm Password	The password associated with the username for this CDN service.
Description	Optional. User defined description for the CDN service.

Step 4 On completion, click **Create**. The CDN is created and a validation message is displayed.

Step 5 Click **Close**.

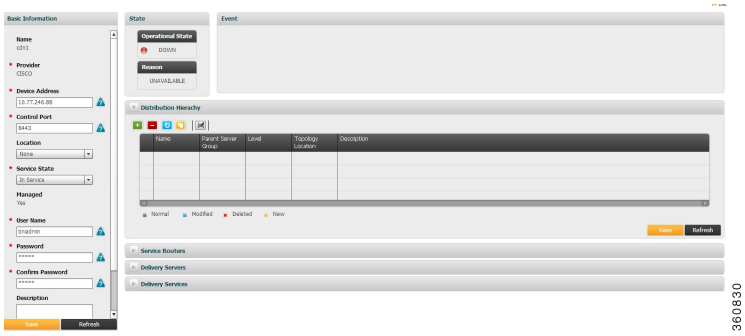
Step 6 From within the CDN screen, click **Refresh** to view the newly added CDN service.
Note that the CDN synchronization will take a few minutes.

Managing a VDS-IS CDN

To manage a VDS-IS CDN, complete the following:

Step 1 From the main page, select **Configuration** > **CDN**.

Step 2 Click on the arrow next to the name of the CDN you want to manage. The Distribution Hierarchy maps to the CDSM location.



The following table provides a description of the key elements contained within the selected CDN page.

Table 94: CDN - Field & Description

Element	Description
Distribution Hierarchy	The Distribution Hierarchy maps to CDSM locations (see Distribution Hierarchy Function Overview, on page 124).
Service Routers	The VDS-SM Service Routers map to the CDSM devices (SRs).
Delivery Servers	The VDS-SM Delivery Servers map to the CDSM devices (SEs) (see Delivery Servers, on page 127).
Delivery Services	The VDS-SM Delivery Services map to the CDSM Delivery Services (see Delivery Services, on page 127).

Distribution Hierarchy Function Overview

Adding a Distribution Hierarchy

To add a Distribution Hierarchy, perform the following steps:

Step 1 From the main page, click **Configuration** > **CDN**.

Step 2 Select the CDN to which you want to add Distribution Hierarchy and click .

Step 3 In the Distribution Hierarchy tab, click .

Step 4 In the dialog box that appears on the right pane, enter the following details:

Table 95: Adding Distribution Hierarchy - Field & Description

Field	Description
Name	Specify the Server Group name.
Parent Server Group	Specify the Parent Server Group.
Topology Location	Specify the Topology Location.
Level	Specify the level to which the Delivery Server belongs.
Description	Optional. Additional information about the Distribution Hierarchy.

Step 5 Click **OK**.

Step 6 Click **Save**.

Modifying a Distribution Hierarchy

To modify a Distribution Hierarchy, perform the following steps:

Step 1 From the main page, select **Configuration** > **CDN**.

Step 2 Select the CDN that you want to modify and click .

Step 3 From the Distribution Hierarchy tab, select the Distribution Hierarchy that you want to modify and click .

Step 4 Enter the modification in the dialog box that appears on the right pane and click **OK**.

Step 5 Click **Save**.

Cloning a Distribution Hierarchy

This feature helps you to replicate an existing Distribution Hierarchy. This is helpful when you want to create the same Distribution Hierarchy again.

Step 1 From the main page, select **Configuration** > **CDN**.

Step 2 Select the CDN that you want to clone and click  .

Step 3 From the Distribution Hierarchy tab, select the Distribution Hierarchy, which you want to clone and click  .

Step 4 Click  and then click **OK**.

Step 5 Click **Save**.

Deleting a Distribution Hierarchy

To delete a Distribution Hierarchy, perform the following steps:

Step 1 From the main page, select **Configuration** > **CDN**.

Step 2 From the Distribution Hierarchy tab, select the Distribution Hierarchy that you want to delete and click  .
You can also undo a task that you have just performed. This option is not feasible for an existing Delivery Hierarchy. For example, you can undo a Distribution Hierarchy, immediately after it has been added. For this, select the task that you want to undo (the task that you just performed), and click  .

Delivery Servers

Modifying a Delivery Server

To modify a Delivery Server, perform the following steps:

Step 1 From the main page, click **Configuration > CDN**.

Step 2 Select the CDN that you want to modify and click  .

Step 3 In the Delivery Servers tab, select the Delivery Server that you want to modify and click  .

Step 4 Enter the modification and click **OK**.

Step 5 Click **Save**.

Note You can only modify the Description and Server Group fields.

Delivery Services

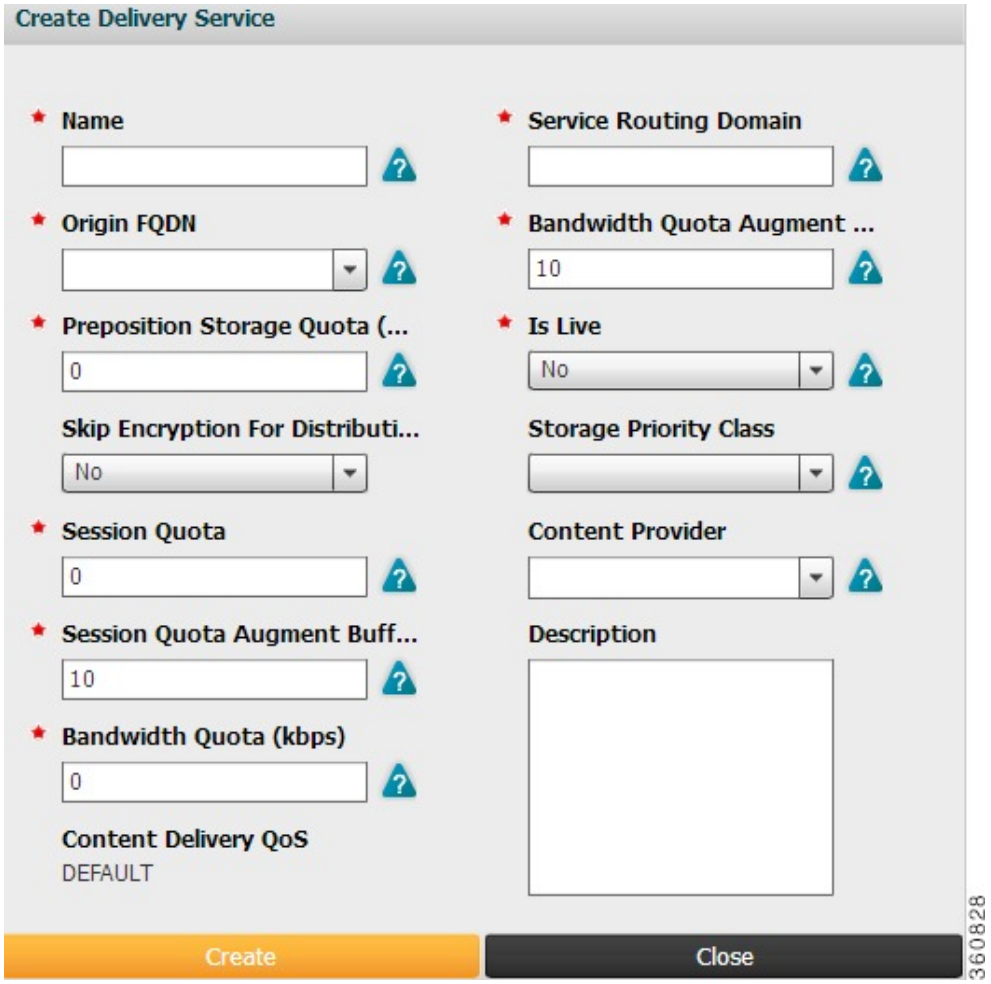
Adding a Delivery Service

To add a Delivery Service, perform the following steps:

Step 1 From the main page, select **Configuration** > **CDN**.

Step 2 Select the CDN to which you want to add a Delivery Service and click  .

Step 3 On the Delivery Services tab, click  .



Step 4 Enter the following details in the Create Delivery Service dialog:

Table 96: Adding Delivery Service - Field & Description

Field	Description
Name	Specify the Delivery Service name.
Origin FQDN	Specify the FQDN of the Content Provider.
Preposition Storage Quota (MB)	Maximum content disk storage size for each SE, in megabytes, for pre-fetched content and metadata, and hybrid metadata for this delivery service. **Note** The Preposition Storage Quota configured does not affect cache content quota size; it only restricts prefetched content storage for each SE. If the total prefetched content storage size is less than the configured quota, then the extra storage is used for dynamic cache files.

Field	Description
Skip Encryption for Distribution	Specify whether you need to skip encryption for distribution. Select **No** for encryption and **Yes** to skip encryption.
Session Quota	Maximum number of concurrent sessions allowed for this delivery service. The default is zero, which means no session limits are set for this delivery service.
Session Quota Augment Buffer (%)	Buffer, as a percentage, of the maximum number of concurrent sessions allowed over the Session Quota. If this threshold is exceeded, no new sessions are created until the number of concurrent sessions is below this threshold. The range is from 0 to 1000. The default is 10.
Bandwidth Quota (kbps)	Maximum bandwidth allowed for this delivery service. The default is zero, which means no bandwidth limits are set for this delivery service.
Content Delivery QoS	This is automatically set as default.
Service Routing Domain	Specify the Service Routing Domain Name.
Bandwidth Quota Augment Buffer (%)	Buffer, as a percentage, of the maximum bandwidth allowed over the Bandwidth Quota. If this threshold is exceeded, no new sessions are created until the bandwidth used is below this threshold. The range is from 0 to 1000. The default is 10.
Is Live	When checked, creates a live program to distribute live or scheduled programs to the SEs associated with this delivery service and with the live program. This delivery service does not have a related Manifest file and cannot be used to distribute file-based content as regular delivery services do. The live program learns about a live stream through a program file that describes the attributes of the program. Checking this check box disables the Delivery Service Quota field and fields in the Acquisition and Distribution Properties section.
Storage Priority Class	Select the correct option from the drop-down list. **Note** This is configured in CDS-IS and is synced automatically.
Content Provider	Associate the delivery service with the content provider.
Description	Optional. Additional information about the Delivery Service.

Step 5 Click **Create**.

Step 6 Verify that the Delivery Service has been created successfully by selecting **Delivery Services** within the CDN page and then verifying that the newly created Delivery Service is present.

Step 7 Click  next to the newly created delivery service to associate delivery servers to it.

Step 8 Display a list of available delivery servers by clicking  .

Step 9 Select one or multiple delivery servers that will be associated to the delivery service. Then, select the delivery server, which will be the Content Acquirer, from the drop-down menu and then click **OK**.

The Content Acquirer can be changed at any time from the main Delivery Service configuration page, using the **Assign Content Acquirer** icon.

Deleting a Delivery Service

Step 1 From the main page, click **Configuration > CDN**.

Step 2 Select the CDN that you want to delete and click  .

Step 3 In the Delivery Services tab, select the Delivery Service that you want to delete.

Step 4 Click  and in the confirmation dialog, click **Yes** to permanently delete the Delivery Service, and click **No** to cancel the deletion.

Reseller Function Overview

A reseller is a user who buys delivery services from CDN and sells to the content providers. A reseller is allocated a specific session bandwidth storage quota.

Adding a Reseller

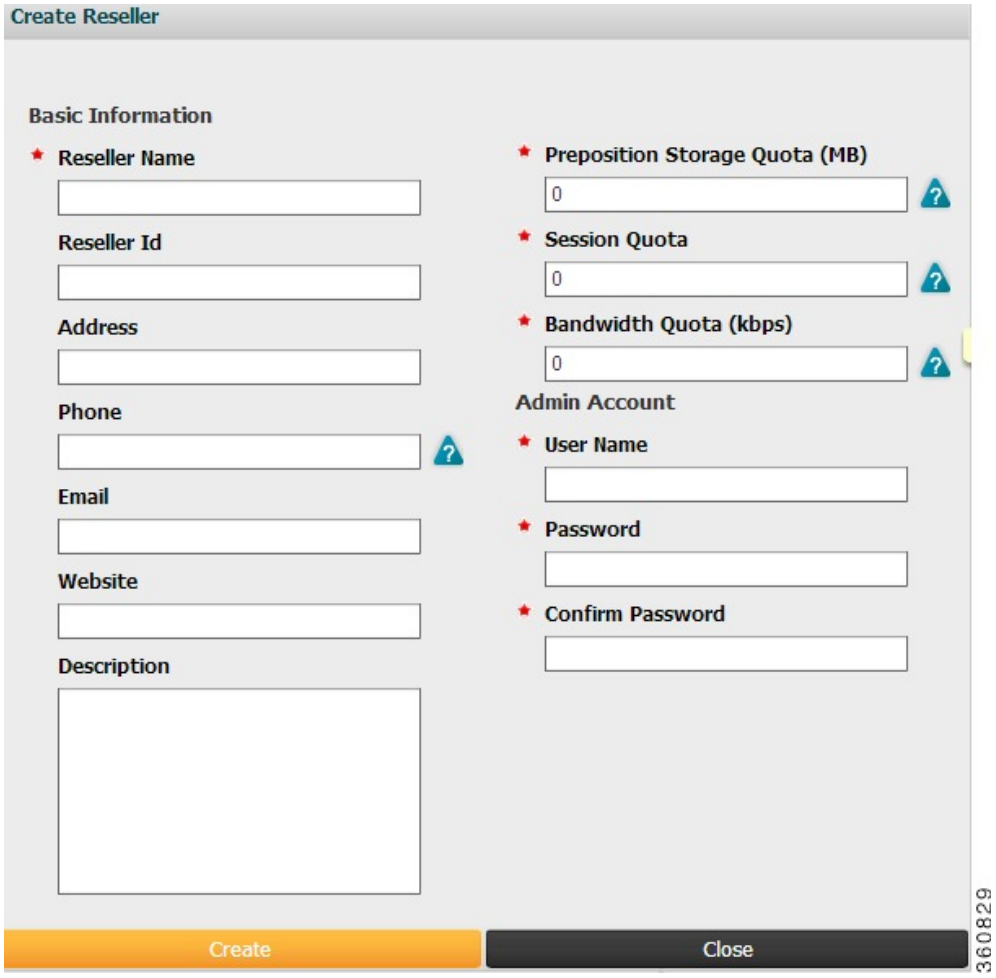
To add a reseller, complete the following:

Step 1 Log in to the application.

Step 2 Enter your username and password.

Step 3 From the main page, select **Configuration** > **Customers** > **Reseller**.

Step 4 Click  to open the **Create Reseller** dialog.



Adding a Reseller involves configuring or modifying the following fields:

Table 97: Adding a Reseller - Field & Description

Field	Description
Reseller Name	Specify a unique name for the reseller.
Reseller Id	Specify the ID for the reseller.
Address	Specify the IP address or FQDN (full qualified domain name) of this reseller.
Phone	Specify the phone number for the reseller.
Email	Specify the email address for the reseller.
Website	Specify the web site URL for the reseller.
Description	Optional. Additional information about the reseller.
Preposition Storage Quota (MB)	Specify the maximum data in MB that can be prepositioned for the reseller.

Field	Description
Session Quota	Specify the maximum number of sessions that can be active for the reseller.
Bandwidth Quota (Kbps)	Specify the maximum bandwidth allowed for the reseller.
User Name	Specify a user name associated with the reseller.
Password	Specify the user's password associated with this reseller.
Confirm Password	Re-enter the user's password associated with this reseller.

Step 5 Click **Create** to add the Reseller.

Modifying a Reseller

To modify a Reseller, perform the following steps:

Step 1 From the main page, select **Configuration** > **Customers** > **Reseller**.

Step 2 Select the Reseller that you want to modify and click  .

Step 3 On the left pane, enter the modification and click **Save**.

Deleting a Reseller

To delete a Reseller, perform the following steps:

Step 1 From the main page, select **Configuration** > **Customers** > **Reseller**.

Step 2 Select the Reseller that you want to delete and click  .

Step 3 Click **Yes** to permanently delete the Reseller, and click **No** to cancel the deletion.

Content Provider Function Overview

A content provider is a user who buys delivery services from CDN and serves the content.

Adding a Content Provider

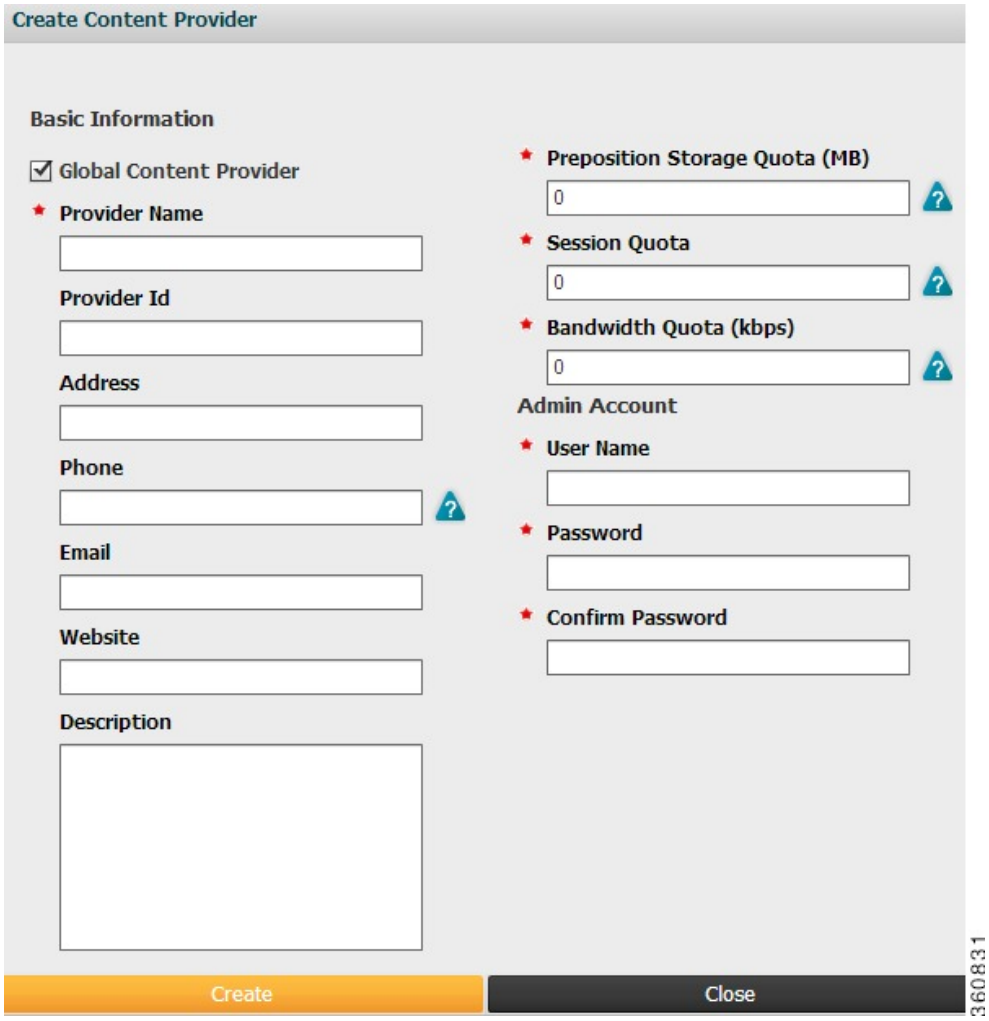
To add a content provider, complete the following steps:

Step 1 Log in to the application.

Step 2 Enter your username and password.

Step 3 From the main page, select **Configuration** > **Customers** > **Content Provider**.

Step 4 Click to open the **Create Content Provider** dialog.



Adding a Content Provider involves configuring or modifying the following fields:

Table 98: Adding a Content Provider - Field & Description

Field	Description
Provider Name	Specify a unique name for the content provider.

Field	Description
Provider Id	Specify the ID for the content provider.
Address	Specify the IP address or FQDN of this content provider.
Phone	Specify the phone number for this content provider.
Email	Specify the email address for this content provider.
Website	Specify the web site URL for this content provider.
Description	Optional. Additional information about the content provider.
Preposition Storage Quota (MB)	Specify the maximum data in MB that can be prepositioned for the reseller.
Session Quota	Specify the maximum number of sessions that can be active for the reseller.
Bandwidth Quota (Kbps)	Specify the maximum bandwidth allowed for the reseller.
User Name	Specify a user name associated with the content provider.
Password	Specify the user's password associated with this content provider.
Confirm Password	Re-enter the user's password associated with this content provider.

A Content Provider that is not a global Content Provider, will be available under the Reseller option. To view the Reseller option, uncheck Global Content Provider. From the Reseller drop-down, choose the Reseller, which you want to associate the Content Provider to.

Step 5 Click **Create** to add the Content Provider.

Mapping a Content Provider and Delivery Service

To map a Content Provider and Delivery Service, perform the following steps:

Before You Begin

Before you map a Content Provider and Delivery Service, you need to first create the Delivery Service in CDN. For this, you need to add CDN (see Adding a CDN, on page 122). After you add CDN, you need to add a Delivery Service (see Adding a Delivery Service, on page 127).

Step 1 From the main page, select **Configuration** > **Customers** > **Content Provider**.

Step 2 Select the Content Provider that you want to assign Delivery Service, and click  .

Step 3 Click  and select the Delivery Service that you need to map.

Step 4 Select the CDN that you want to map and click  .

Step 5 Click **Save**.
If you want to assign multiple Content Providers to a single Delivery Service, you must not map Content Provider and Delivery Service.

Assigning Multiple Content Providers to a Single Delivery Service

This feature enables the user to set up multiple Content Providers to a single Delivery Service. This is feasible by providing custom Regex option, wherein the CDN Operator can provide the Regex for new field CP_ID. This custom regex is used to extract CP_ID from the URL and then perform a lookup to get a meaningful CP name. If the CDN Operator needs to use Asset ID to obtain meaningful CP name, then the Asset ID and CP_ID will have the same Regex for token extraction from the URL. CDN Operators can either create or update Regex for CP_ID extraction. Regex is maintained in props.conf, a Splunk configuration file.

To create or update Regex for CP_ID, perform the following steps:

Step 1 Log in to the analytics JS node using the following credentials:
Username: **bnisplunk**

Password: **password**

Step 2 Execute the script configure_regex.py using the following command to add/update:
$SPLUNK_HOME/bin/splunk cmd python $SPLUNK_HOME/etc/apps/CDN_JS/bin/configure_regex.py add <sourcetype> <fieldname> "<regex>"

Where, <sourcetype> is the sourcetype for which the regex is provided.

The valid source types are: fms_disconnect, wmt_logplaystats, we_access, abr_session and sr_transaction

<regex>—regex to extract the Content Provider information from the log data

<fieldname>—the valid field names are CP_ID and Asset

Example:
For the following log file entry:

[28/Nov/2012:23:54:42.315+0000] 1799 74.126.71.217 TCP_HIT/206 2458 GET http://ccp-cmc-smooth-localpod02-linear.cdn2.net/content/CP1/hls/file0/file_500.m3u8 application/x-mpegURL - hls 0 - 2012112910000000010000000 1 [29/Nov/2012:00:00:02.317+0000] External –

Case1: If you want to extract content/CP1 as CP_ID, then the Regex is:

"(?i)^(?:[^]*({1,2})){6}(?:[a-z]+://)(?:[^ /:]+[^ /]+/)(?P<CP_ID>[^ /]+/[^ /]+)"

Case 2: If you want to extract CP1 as CP_ID, then the Regex is:

"(?i)^(?:[^]*({1,2})){6}(?:[a-z]+://)(?:[^ /:]+[^ /]+/[^ /]+/)?(?P<CP_ID>[^ /]+)"

Case 3: If you want to extract file_500.m3u8 as Asset, then the Regex is:

"(?i)^(?:[^]*({1,2})){6}(?:[a-z]+://)(?:[^ /:]+[^ /]+/[^ /]+/[^ /]+/[^ /]+/[^ /]+/)(?P<Asset>[^]+)"

Once this script is executed, redeployment of the server is initiated automatically.

To delete Regex for CP_ID, use the following command:

#$SPLUNK_HOME/bin/splunk cmd python configure_regex.py <remove> <sourcetype> <fieldname>

Modifying a Content Provider

To modify a Content Provider, perform the following steps:

Step 1 From the main page, select **Configuration** > **Customers** > **Content Provider**.

Step 2 Select the Content Provider that you want to modify and click  .

Step 3 In the left pane, enter the modification and click **Save**.

Deleting a Content Provider

To delete a Content Provider, perform the following steps:

Step 1 From the main page, select **Configuration** > **Customers** > **Content Provider**.

Step 2 Select the Content Provider that you want to delete and click  .

Step 3 Click **Yes** to permanently delete the Content Provider, and click **No** to cancel deletion.

Services

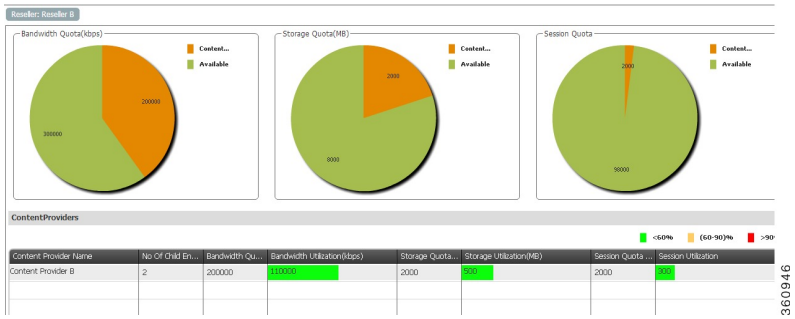
This feature provides a quick overview of the bandwidth, session, and storage quota for each reseller, content provider, and delivery service in the CDN to the CDN Operator. Theses quotas need to be specified when you create delivery service, content provider, and reseller.

To access this feature, from the main page, click **Configuration** > **Services**.

On the right pane, the overall CDN allocation is displayed.

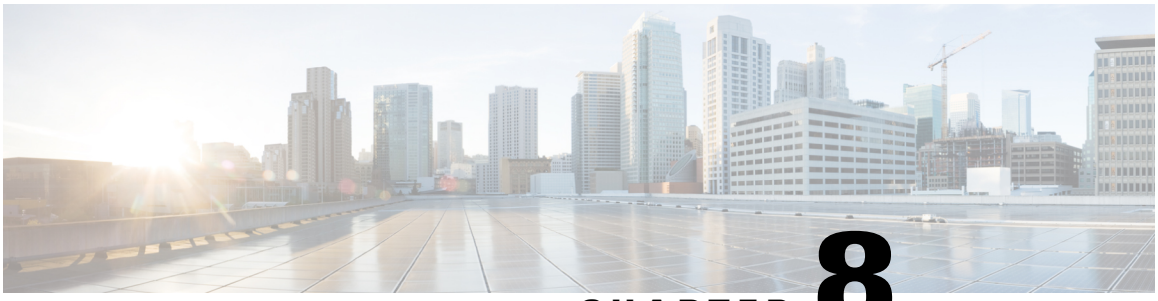
To view the bandwidth, session, and storage quota for each reseller, click the arrow next to CDN. The resellers under the CDN are displayed. Select a specific reseller to view the allocation.

To view the bandwidth, session, and storage quota of each content provider, click the arrow next to the respective reseller. The content providers under the resellers are displayed. Select a specific content provider to view the allocation.



To view the delivery services of each content provider, click the arrow next to the respective content provider. The delivery services under the content providers are displayed.


Configuration / Services
CDN
Reseller A
CP1
HBO
CNN
ESPN
Movies-VOD
CP2
CP3
Reseller B
Reseller C
Content Provider - CP1
Bandwidth Quota
Session Quota
Storage Quota
HBO
CNN
ESPN
Movies-VOD
Available
Delivery Service
Type
Bandwidth Quota
Bandwidth Usage
Storage Quota
Storage Usage
Session Quota
Max Concurren...
HBO LIVE 30 25 30 20 30 15
CNN LIVE 15 5 15 15 15 8
ESPN LIVE 25 15 25 12 25 20
Movies-VOD VOD 30 10 30 25 30 15
360311



CHAPTER 8

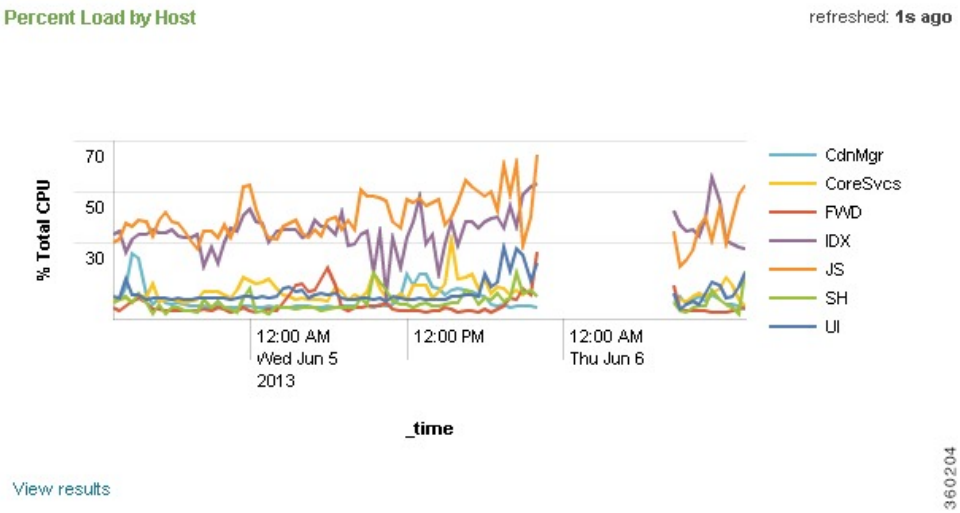
Administration

System Load Dashboard

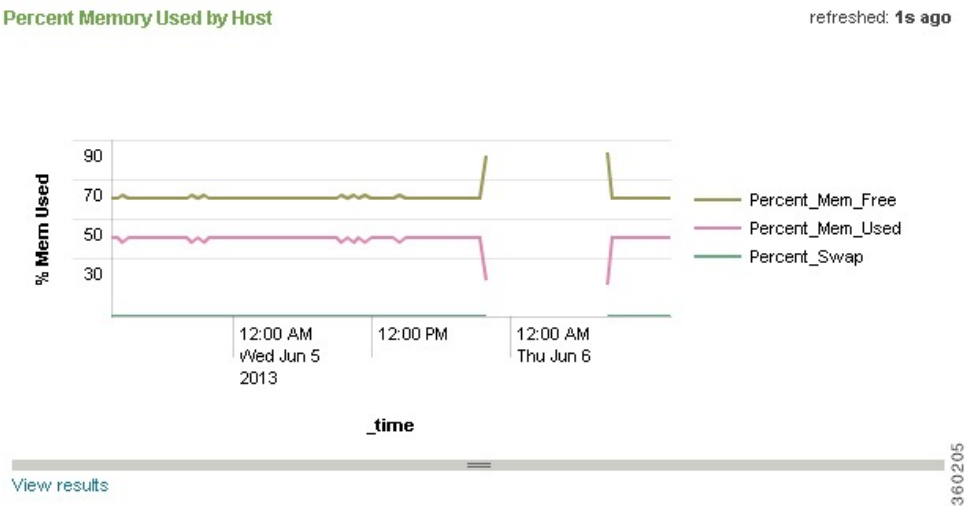
Displays charts that represents Percent Load by Host, Percent Memory Used by Host , Disk Used by Host and Volume, and Interface Throughput, across the nodes in the system.

To access System Load Dashboard, from the main page, click **Administration** > **System Load Dashboard**.

Percent Load by Host

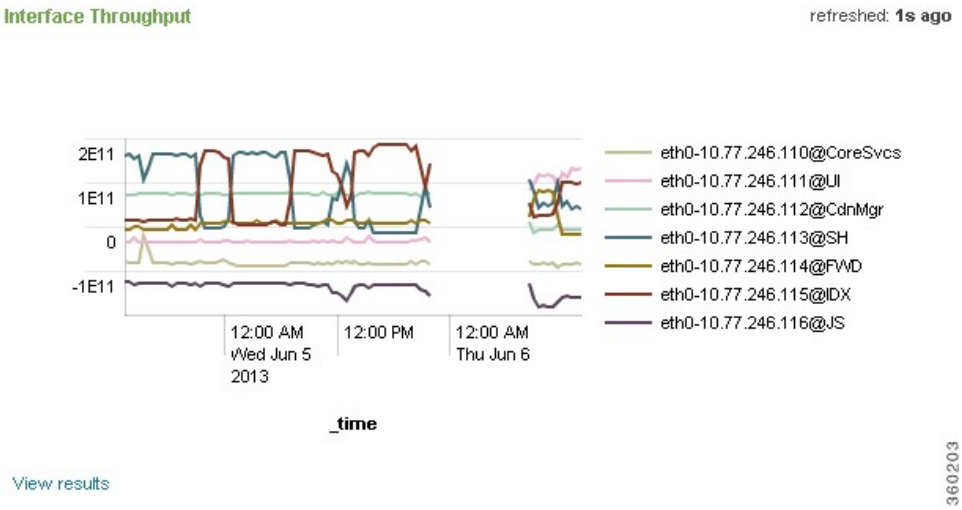


Percent Memory Used by Host



Disk Used by Host and Volume

Interface Throughput



Managing Users and Roles Overview

Administrators can create specific users and set their roles from the **User Management** page.

To access User Management, from the main page, click **Administration** > **User Management**. In this feature, you can add and delete a user.

About User Accounts

User accounts define user roles and access privileges to system configuration and management functional areas.

The CDN Manager includes a default user profile with Cisco Administrator access privileges, to provide the Network Administrator first-time access to the CDN Manager system.

Administrator privileges provide full rights to all system functions. You must have Administrator privileges to define roles and grant access permissions to system functions.

Note For added security, we recommend that you replace the Cisco Administrator account with a new Administrator user account, specific to only your network management.

Roles

A user's role dictates the functional area and level of access that is granted to the user.

Following is a list of the supported roles:

- CDN Operator Administrator
- CDN Operator Viewer

- Reseller Administrator
- Reseller Viewer
- Content Provider Administrator
- Content Provider Viewer

Adding a User

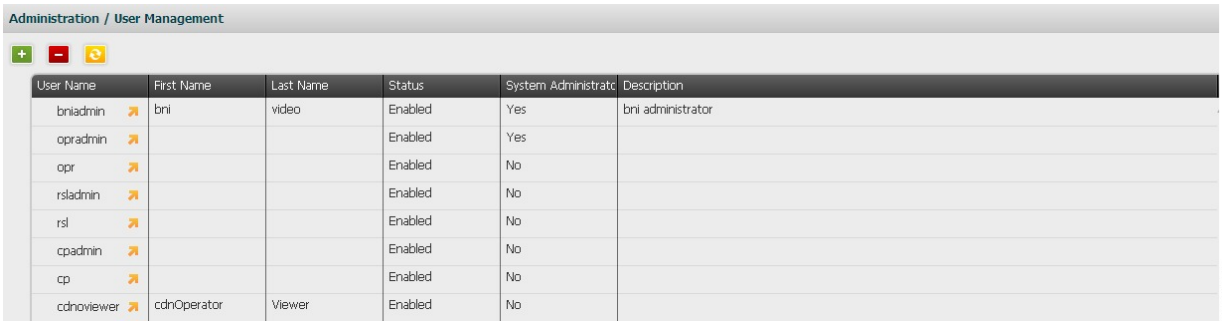
Adding a user involves:

- Creating the user
- Defining the user's role

Note You must have Administrator rights to add a user.

To add a user:

Step 1 From the main page, click **Administration** > **User Management**.



Step 2 Click to add the user and define the user's role.

Step 3 In the Create New User dialog, type the values in the fields or select an option from the drop-down menu.

Step 4 Add the user's name and password. By default, the role is set to Admin.

Step 5 Click **Create**.

Deleting a User

To delete a user, perform the following:

Step 1 From the main page, click **Administration** > **User Management**.

Step 2 From the User Management page, select the user you want to delete.

Step 3 Click  .

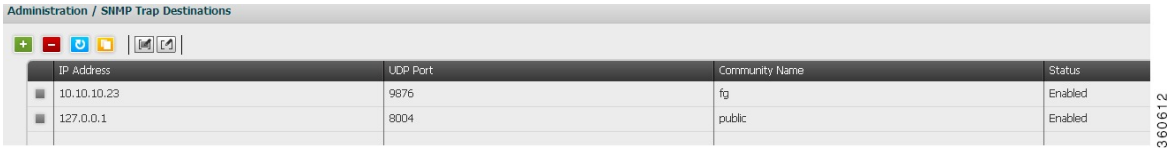
Step 4 Click **Yes** in the confirmation dialog.
The user will be deleted.

SNMP Trap Destinations

The SNMP Trap Destinations function monitors solution nodes and operational status.

The SNMP trap destination contains the information that the SNMP agent sends as notifications to an SNMP manager. This information includes the IP Address, UDP Port, Community Name (Community String), and the Status.

To access SNMP Trap Destinations, from the main page, click **Administration** > **SNMP Trap Destinations**. This feature enables you to add and delete SNMP Trap Destinations.



Adding SNMP Trap Destinations

To add SNMP Trap Destinations, perform the following steps:

Step 1 From the main page, click **Administration** > **SNMP Trap Destinations**.

Step 2 Click  and enter the details in the dialog that appears.

Step 3 Click **OK** and then, click **Save**.

Deleting SNMP Trap Destinations

To delete SNMP Trap Destinations, perform the following steps:

Step 1 From the main page, click **Administration** > **SNMP Trap Destinations**.

Step 2 Select the SNMP Trap Destination information, which you want to delete.

Step 3 Click  .

Step 4 Click **OK** and then, click **Save**.
The SNMP Trap Destination information will be deleted.

Global Configurations

Configuration includes any settings that exist on an *Appliance*, which an end-user might modify in the following ways:

- Using the Appliance Agent (rAPA) User Interface (UI) or Manager User Interface
- A manual edit to a specific file using a documented procedure; for example, file system modification of jboss-log4j.xml or workflows
- By copying a modified file onto the appliance from elsewhere

Important! Modifying a Global Configuration can have a major impact on the running system. A parameter change should only be made by a System Administrator who has a detailed understanding about the impact of the change on the running system.

A baseline configuration is established at the conclusion of installing each appliance. Any parameters not mentioned in this document (for example, tty device definitions) should be considered non-modifiable.

The following lists the configuration parameter elements:

- **Configuration Elements**: Kinds of configuration settings used by the system; for example, topology or configuration database, SNMP, workflow, and so on.
- **Appliance Configuration Parameters**: Summary of all parameters used in configuring appliances with description, value type, and so on.
- **Solution Node Settings**: Settings recorded on each node, which define that node's specific role in the overall solution.
- **Global Configuration Settings**: Globally visible configuration sections, each containing a description of all parameters in the section, including the product defaults.
- **System Topology**: Topology data and its usage, import/export operations and the export schema.
- **Configuration Files**: Essential files for each appliance that contain the configuration for the appliance.

  To access Global Configurations, click **Administration** > **Global Configurations**.

Adding Global Configurations

To add global configurations, perform the following:

Step 1 From the main page, click **Administration** > **Global Configurations**.

Step 2 Click  to add global configurations.

Step 3 Enter the details and click **OK** and then click **Save**.

Deleting Global Configurations

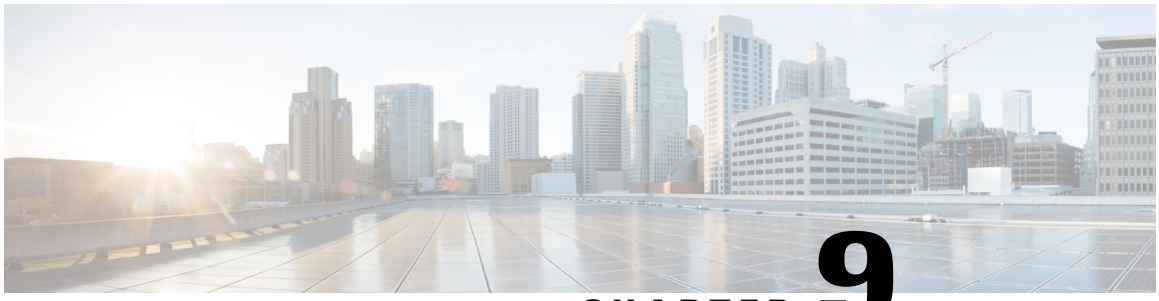
To delete global configurations, perform the following:

Step 1 From the main page, click **Administration** > **Global Configurations**.

Step 2 Select the Global configuration you want to delete.

Step 3 Click  .

Step 4 Click **OK** and then click **Save**.



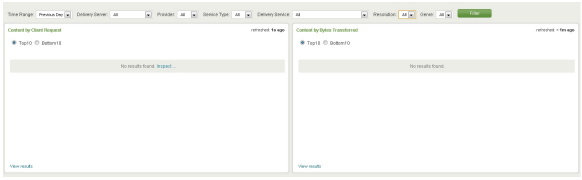
CHAPTER 9

Troubleshooting

Troubleshooting Analytics Dashboards

The analytics system is a critical tool for troubleshooting run-time issues, as well as providing trending information that can be used for capacity planning and other purposes. If it is not properly operating, the ability to use it for troubleshooting is lost.

The most commonly observed behavior of the analytics system that is not working, is a lack of data. If any of the above functions are not operating properly, the Dashboards and Reports data may not appear, and the message “no result found” is displayed.



The following list provides possible problems that could arise while using the VDS Analytics:

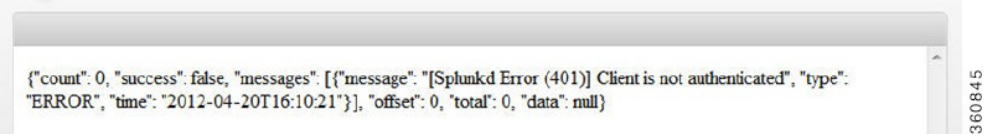
- Splunk licensing
- Splunk Forwarder not operating correctly
- Analytics Indexer not operating
- Search Head not operating

Troubleshooting Splunk Licensing Issues

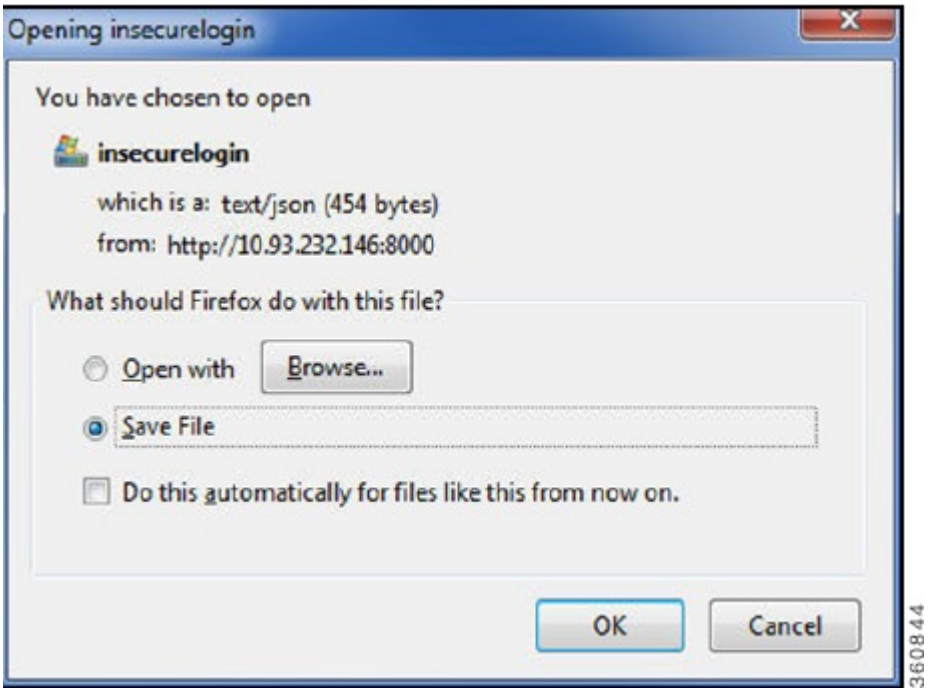
Depending on the browser being used, either Internet Explorer (IE) or Firefox, Splunk licensing issues may cause different errors to appear.

The following are examples of a Splunk licensing errors.

- Splunk licensing issues in IE.



- Splunk licensing issues in Firefox. In Firefox, an insecurelogin file will start to download. For example:



If a Splunk licensing issue occurs, use the following procedure to create a new Splunk license.

Step 1 Copy the Splunk license file to your local machine, taking care to note the location, which will be used later in this procedure.

Step 2 Open the Splunk manager app on the Job Scheduler. Using the following:

Example:
`http://<IP of Job Sched>:8000/en-us/manager`
Username: **Admin** or **admin**

Example:

Password: **Beaumaris1**

Step 3 Select **Licensing**.

Step 4 Select **Add License**.

Step 5 Browse your machine to the location where you copied the license file. **Note:** Do not change the filename.

Step 6 Select **Install**.

Step 7 Return to the Licensing page and confirm whether the new license is added and is valid.

Troubleshooting Splunk Forwarder Issues

Step 1 SSH to the Forwarder.

Step 2 Login to the Forwarder using, username: **bninet** and password: **password**.

Step 3 At the Forwarder prompt, enter the PS command to verify that the Splunk Forwarder is running. For example:

Example:
[bninet@FW ~]$ **ps eax | grep splunkd | grep 8088**

2256 ? Sl 0:52 splunkd -p 8088 start CONSOLE=/ dev /console SELINUX_IN IT=YES SHELL=/bin/bash TERM= linux USER= bninet INIT_VERSION=sysvinit-2.86 PATH=/h ome / bninet / splunkforwarder /bin:/ sbin :/ usr / sbin :/bin:/ usr /bin _=/home/ bninet / splu nkforwarder /bin/ splunk runlevel =3 RUNLEVEL=3 PWD=/ LANG=en_US.UTF-8 previous=N P REVLEVEL=N SHLVL=3 HOME=/home/ bninet LOGNAME= bninet HOSTNAME=FW SPLUNK_HOME=/ hom e/ bninet / splunkforwarder SPLUNK_DB=/home/ bninet / splunkforwarder / var /lib/ splunk S PLUNK_SERVER_NAME= splunkforwarder SPLUNK_WEB_NAME= splunkweb LD_LIBRARY_PATH=/ hom e/ bninet / splunkforwarder /lib LDAPCONF=/home/ bninet / splunkforwarder / etc / openldap / ldap.conf

2257 ? Ss 0:04 splunkd -p 8088 start CONSOLE=/ dev /console SELINUX_IN IT=YES SHELL=/bin/bash TERM= linux USER= bninet INIT_VERSION=sysvinit-2.86 PATH=/h ome / bninet / splunkforwarder /bin:/ sbin :/ usr / sbin :/bin:/ usr /bin _=/home/ bninet / splu nkforwarder /bin/ splunk runlevel =3 RUNLEVEL=3 PWD=/ LANG=en_US.UTF-8 previous=N P REVLEVEL=N SHLVL=3 HOME=/home/ bninet LOGNAME= bninet HOSTNAME=FW SPLUNK_HOME=/ hom e/ bninet / splunkforwarder SPLUNK_DB=/home/ bninet / splunkforwarder / var /lib/ splunk S PLUNK_SERVER_NAME= splunkforwarder SPLUNK_WEB_NAME= splunkweb LD_LIBRARY_PATH=/ hom e/ bninet / splunkforwarder /lib LDAPCONF=/home/ bninet / splunkforwarder / etc / openldap / ldap.conf

[bninet@FW ~]$

Step 4 If Splunk Forwarder is not running, restart it by using the following command. In the following example, a Splunk Forwarder restart example is shown.

Example:
/ etc / init.d / splunkforwarder restart

Restarting Splunk ...

Password:

Stopping splunkd ...

Shutting down. Please wait, as this may take a few minutes.

. [OK]

Stopping splunk helpers...

[OK]

Done.

Splunk > Needle. Haystack. Found.

Checking prerequisites...

Checking mgmt port [8088]: open

Checking conf files for typos...

All preliminary checks passed.

Starting splunk server daemon (splunkd)...

[OK]

Done.touch : cannot touch `/ var /lock/ subsys / splunk ': Permission denied

If the nodes are forwarding, there should be constant updates in the splunkd log file located in "/opt/splunkforwarder/var/log/splunk". If the processes are running and the log is not being updated, contact Cisco Customer Support.

Troubleshooting the Splunk Indexer

Step 1 ssh into the IP address of the Indexer.

Step 2 Using the **netstat** command, list the monitoring ports. For example:

Example:
[bninet@IDX **netstat -a 2>>/ dev /null | grep 8089t**

tcp 0 0 *:8089 *:* LISTEN

[bninet@IDX ~]$

Step 3 If there are no jobscheduler processes listening on port 8089, then the indexer is not functioning. Restart the indexer. For example:

Example:
[bninet@IDX ~]$ **sudo / etc / init.d / splunk restart**

Restarting Splunk ...

splunkweb is not running.

Stopping splunkd ...

Shutting down. Please wait, as this may take a few minutes.

..... [OK]

Stopping splunk helpers... [OK]

Done.

Splunk > The IT Search Engine.

Checking prerequisites...

Checking mgmt port [8089]: open

Checking configuration... Done.

Checking index directory...

Validated databases: _audit _ blocksignature _internal _ thefishbucket cdn-mgr cdnmanager cms dsm history main os summary

Done

Bypassing local license checks since this instance is configured with a remote license master.

Success

Checking conf files for typos...

All preliminary checks passed.

Starting splunk server daemon (splunkd)...

[OK]

Done.

Troubleshooting the Analytics Search Head

To verify that the Analytics Node (often referred to as the search head) is operating properly, complete the following:

Step 1 ssh into the IP address of the analytics node.

Step 2 Using the **netstat** command, list the monitoring ports. For example:

Example:
[bninet@IDX **netstat -a 2>>/ dev /null | grep 8089**

tcp 0 0 *:8089 *:* LISTEN

[bninet@IDX ~]$

Step 3 If there are no analytics node processes listening on port 8089, then the nodes are not functioning. Restart Splunk. For example:

Example:
[bninet@IDX ~]$ **sudo / etc / init.d / splunk restart**

Restarting Splunk ...

splunkweb is not running.

Stopping splunkd ...

Shutting down. Please wait, as this may take a few minutes.

..... [OK]

Stopping splunk helpers... [OK]

Done.

Splunk > The IT Search Engine.

Checking prerequisites...

Checking mgmt port [8089]: open

Checking configuration... Done.

Checking index directory...

Validated databases: _audit _ blocksignature _internal _ thefishbucket cdn-mgr cdnmanager cms dsm history main os summary

Done

Bypassing local license checks since this instance is configured with a remote license master.

Success

Checking conf files for typos...

All preliminary checks passed.

Starting splunk server daemon (splunkd)...

[OK]

Done.

In addition, the command **sudo /home/ bninet /splunk/bin/splunk search 'index= dsm | stats count' - auth admin:changeme** can be run to show that the analytics node is capable of processing data from the indexer, as shown below. This command sends scrolling data to the screen, which is compressed in the output below:

Example:

[bninet@Search ~]$ /home/bninet/splunk/bin/splunk search 'index= dsm | stats count' -auth admin:changeme

count

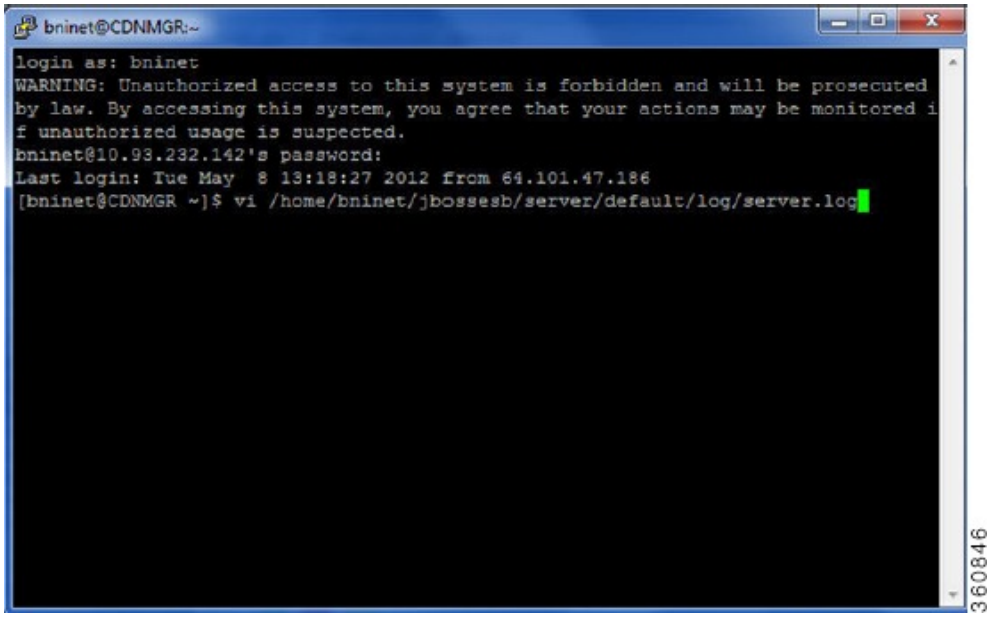
0

Troubleshooting VDS-IS Provisioning

The server.log file, located within the /home/bninet/jbossesb/server/default/log/ folder, can be used to troubleshoot VDS-IS provisioning problems.

To access the server.log file, perform the following step:

ssh into the CDN Manager node and then enter the following command:
`/home/bninet/jbossesb/server/default/log/server.log`



Deleting Summarized Data

To delete the summarized data, perform the following:

Step 1 Launch the JS node web interface http://<JSipaddress>:8000

Step 2 Login to the Splunk web interface by providing the credentials; Username: **admin** and Password: **Beaumaris1**

Step 3 Select **App** and then select **Search**

Step 4 Execute the search query [index=summary report="<Report Name>" host="<JS Host Name>" | delete]
Provide the appropriate report name and hostname in the query.

Example:
[index=summary report=mobitv_client_daily host= secondary-JS | delete]

Step 5 Validate the count by issuing the search query [index=summary report=mobitv_client_daily]

Note can_delete role is already added for Admin. However, the above query will not work in a normal search page.

Splunk License Violation

Violations occur when you exceed the maximum indexing volume allowed for your license. If you exceed your licensed daily volume on any one calendar day, you will get a violation *warning*. The message persists for 14 days. If you have 5 or more warnings on an Enterprise license or 3 warnings on a Free license in a rolling 30-day period, you are in *violation* of your license and search will be disabled.

Note Summary index volume is not counted against your license.

If you get a violation warning, you have until midnight (going by the time on the license master) to resolve it before it counts against the total number of warnings within the rolling 30-day period.

During a license violation period:

- Splunk does not stop indexing your data. Splunk only blocks search while you exceed your license.
- Searches to the _internal index are not disabled. This means that you can still access the Indexing Status dashboard or run searches against _internal to diagnose the licensing problem.

For any queries on licensing, contact the Cisco Accounting team.