Media Broadcaster Release 3.14 User Guide

First Published: 2018-06-25

Last Modified: 2019-05-09

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

CONTENTS

PREFACE

Preface vii

Audience vii

Conventions vii

CHAPTER 1

Cisco Media Broadcaster Overview 1

Cisco Media Broadcaster Overview 1

MC-Controller 3

MC-Sender 4

MC-Receiver 4

Channel Lineup 5

Broadcasting Groups 5

Media Broadcaster HA Architecture 5

MC-Controller HA Solution 6

HA for Broadcaster Configuration Manager 6

HA for Multicast Controller Manager 6

HA for Stream Status Receiver 7

MC-Sender HA Solution 7

Cisco OMD Director 8

CHAPTER 2

Cisco OMD Director Overview 9

Accessing OMD Director 9

OMD Director HA 9

Log in to OMD Director 10

Logging Out of OMD Director 11

OMD Director User Interface Elements 11

OMD Director Navigation Panel: Monitor Overview 13

Monitor > Server Metrics 13
Monitor > Alarms 13
OMD Director Navigation Panel: Administration 14
OMD Director Navigation Panel: Support 14
OMD Director Navigation Panel: Media Broadcaster > Broadcasting Groups 17
OMD Director Navigation Panel: Media Broadcaster > Insights 18

CHAPTER 3 **Configuring Broadcasting Groups** 19
Add a Broadcasting Group 19
Configure a Broadcasting Group 22
Define the Channel Lineup 22
Configure the Filtering Rules 27
Configure Advanced Settings 29

CHAPTER 4 **Managing Broadcasting Groups** 33
Managing Broadcasting Groups Overview 33
View Existing Broadcasting Groups 34
Add a Broadcasting Group 36
Edit a Broadcasting Group 36
Edit the Channel Lineup 37
Edit the Filtering Rules 39
Add Multicast URL Regex Entries 39
Edit Multicast URL Regex Entries 39
Delete Multicast URL Regex Entries 40
Add an Allowed Server 40
Edit an Allowed Server 41
Delete an Allowed Server 41
Edit the Advanced Settings 41
Export the Channel Lineup 45
Delete a Broadcasting Group 46

CHAPTER 5 **Media Broadcaster Monitoring** 49
Server Metrics 49
Change Time Range and Interval 51

Shift Time and Zoom Time 52
Mouse Over 52
Alarms 53
View Active Alarms 53
Acknowledge an Alarm 54
Search for an Alarm 56
Filter an Alarm 56
Alarms History 57
Filter Alarms History 57
Configure Alarm Rules 58
Create New Alarm Rule 59
Edit an Alarm Rule 61
Deactivate an Alarm Rule 62
Mute Alarms 62

CHAPTER 6 **Media Broadcaster Insights** 65
Multicast Sending Charts 65
Multicast Receiving Charts 67

CHAPTER 7 **OMD Director Administration** 71
Users/Organizations 71
Add a New User 72
Edit an Exiting User 75
Delete a User 76
Reset a User Passphrase 76
Backup Management 78
Schedule Backups 78
Change Schedule 79
Enable/Disable a Scheduled Backup 80
Manually Back Up and Restore a Database 80
Backup Settings 81
Add Remote Backup Destinations 81
Edit or Delete a Remote Backup Destination 83
Add a New Database Backup 83

Edit a Database Configuration 84
User Profile 84
Change User Settings 85
Notification Settings 86
Activity Log 88

APPENDIX A **Appendix: Cisco Media Broadcaster Log Files 91**
Log File Locations 91
Media Broadcaster Statistics: Multicast Receiver 91
Media Broadcaster Statistics: Multicast Sender 92

APPENDIX B **Cisco Media Broadcaster Troubleshooting 93**
Multicast Receiver Joins Multicast but no UDP Packets are Received at Socket Receive Buffers 93
Gateway does not Start the Multicast Receiver 93
Multicast Sender Unable to Acquire Content in a VPLS Network 93

APPENDIX C **Appendix: OMD Director Alarms and Remediation 95**
Media Broadcaster Checks and Thresholds 96
Common and OMD Monitor Checks and Thresholds 100
Media Broadcaster Alarm Remediation Steps 108

Preface

The Cisco Media Broadcaster User Guide provides information on how to use OMD Director to provision and manage Cisco Media Broadcaster.

This preface describes who should read the Cisco Media Broadcaster User Guide, how it is organized, and its document conventions. It contains the following sections:

- Audience, on page vii
- Conventions, on page vii

Audience

This guide is intended to be used by networking professionals that manage the Cisco Media Broadcaster solution.

Conventions

This document uses the following conventions.

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Indication
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

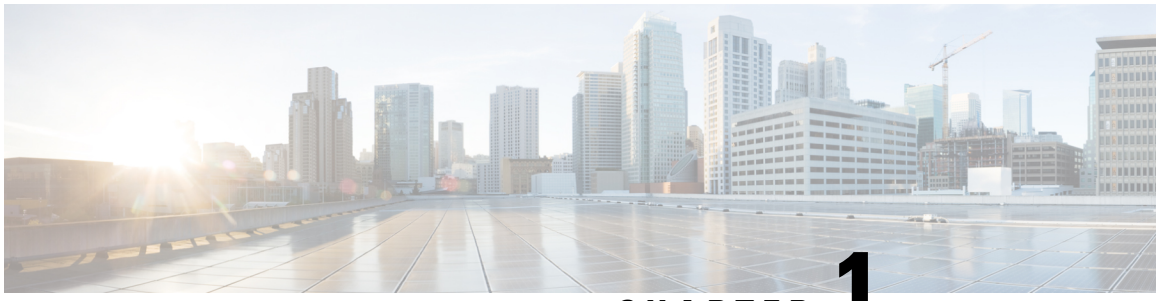
Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS



CHAPTER 1

Cisco Media Broadcaster Overview

This chapter describes the Cisco Media Broadcaster solution, which is part of the Cisco Open Media Distribution (OMD) Suite. This chapter includes the following sections:

- Cisco Media Broadcaster Overview, on page 1
- MC-Controller, on page 3
- MC-Sender, on page 4
- MC-Receiver, on page 4
- Channel Lineup, on page 5
- Broadcasting Groups, on page 5
- Media Broadcaster HA Architecture, on page 5
- Cisco OMD Director, on page 8

Cisco Media Broadcaster Overview

The Cisco Media Broadcaster solution transforms unicast video into multicast data that is distributed across network routers to achieve broadcast-efficient video distribution, which provides service providers a cost-effective scalable solution for streaming HTTP Live adaptive bit rate (ABR) video to in-home primary screens. Cisco Media Broadcaster integrates with an existing ABR delivery system without the need to modify the ABR clients or the video headend components, such as the encoder, packager, and content delivery network (CDN).

The Media Broadcaster solution ingests unicast video from the origin servers or CDN, converts the unicast video stream into a multicast data stream, and distributes it to the home router or set-top box (STB) of the managed homes. The home router or STB converts the multicast data stream back to unicast video. The Media Broadcaster solution is implemented to be fully transparent to both the ABR client and the ABR headend.

Because the Media Broadcaster solution is independent of the existing video delivery infrastructure, it can be integrated with any existing video headend or CDN provider. The solution is highly available and scalable and can support millions of viewers at once. The Media Broadcaster solution offers the following benefits:

- Efficient live ABR video distribution to stream to millions of homes using one IP multicast session
- Cost reduction, which enables convergence to all ABR headend and all ABR clients
- Transparent deployment with no change to the ABR video headend infrastructure, CDN, or ABR players
- Reliable transmission with Forward Error Correction (FEC) or unicast retransmit

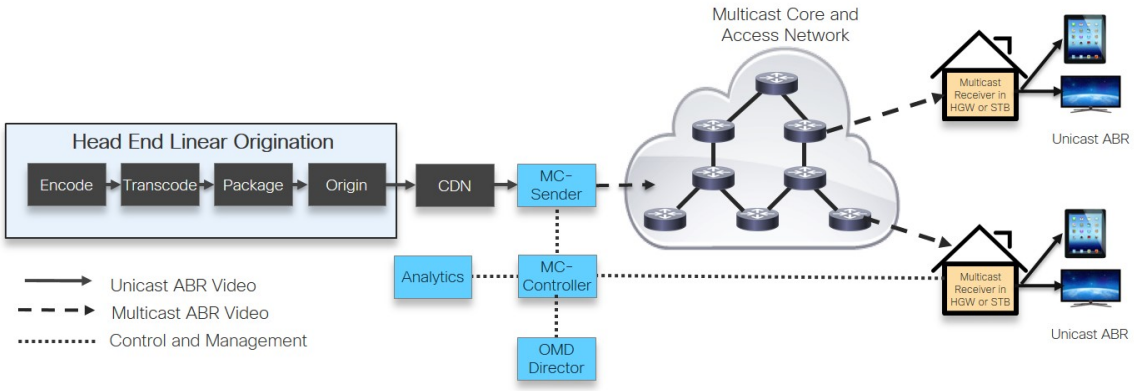
- Optimized network capacity utilization for significant reduction of CDN resources compared to unicast ABR
- Support for IPv4, IPv6, IGMPv3, and IGMPv4 to be compatible with existing multicast standards and networks
- Flexible customer premises equipment (CPE) strategy with the ability to integrate the MC-receiver client into an STB or HGW
- Rapid channel change using unicast client buffer filling from CDN or MC-receiver cache

The primary components of a Cisco Media Broadcaster solution are:

- **OMD Director:** Cisco OMD Director is the primary user interface for the Cisco Media Broadcaster solution. It provides a unified interface to seamlessly manage the different components of the Media Broadcaster platform. OMD Director enables the administrator to rapidly configure Broadcasting Groups, including channel lineups and filtering rules, and integrates monitoring into a single management tool.
- **Multicast Controller (MC-Controller):** The MC-Controller receives the configuration data for channels and overall system settings (including MC-Receiver configuration and multicast configuration) from OMD Director or a northbound interface, and communicates this configuration data to the other components in the system. The MC-Controller also collects info messages, including statistics and status information from MC-Receiver devices.
- **Multicast Sender (MC-Sender):** The MC-Sender is responsible for retrieving ABR content from the CDN and delivering it to the MC-Receivers as multicast streams.
- **Multicast Receiver (MC-Receiver):** The MC-Receiver is located on a customer premise equipment (CPE) device that resides at the managed home of the service provider (either a gateway or a STB) and consists of the proxy service and the Multicast Receiver.
- **OMD Insights:** OMD Insights is an application that provides deep analytics of the Media Broadcaster environment. It is based on Splunk and aggregates data from logs located on the MC-Controllers and MC-Senders. This enables OMD Insights to provide comprehensive Media Broadcaster operational analytics, including analysis of fetch times, network utilization, and efficiency of video content delivery.
- **OMD Monitor:** OMD Monitor is an application that provides in-depth server monitoring, thresholdcrossing, and alarming based on CPU utilization, port utilization, temperature, disk I/O, and other detailed server metrics.

Note All of the components in the Cisco Media Broadcaster solution are designed specifically to interoperate with any CDN, provided that the content is formatted correctly.

The following diagram shows the high-level Media Broadcaster topology and main components. In it, the MC-Sender and MC-Controller reside on separate systems, which provides scalability and reliability. This is the recommended configuration for production Cisco Media Broadcaster deployments. For lab deployments and proof of concept deployments, the MC-Sender and MC-Controller can reside on the same system to save resources.



MC-Controller

The MC-controller is an application that runs on a Linux operating system (bare metal, virtualized, or containerized) in the service provider premise. The main functions of the MC-Controller are:

- Distributes the configuration data to the Multicast Sender (MC-Sender) and Multicast Receiver (MC-Receiver).
- Collects stream status messages from MC-Receivers. These messages include channel viewing and streaming statistics.
- Communicates the channel lineup, which defines which streams to distribute on which multicast addresses, to the MC-Senders.
- Communicates to the MC-Receivers which streams to join and the associated multicast addresses (channel lineup).
- Provides two approaches to determine when to multicast a stream: policy-based or popularity-based. The policy-based approach statically configures a stream to multicast; it does not depend on a certain number of viewers to requesting the stream. The popularity-based approach enables streams to start and stop multicasting based on crossing configured concurrent viewer thresholds.
- Exports data to a Cisco Media Broadcaster element management system.

The MC-Controller contains the following subcomponents:

- **Broadcaster Configuration Manager (BCM):** The BCM retrieves and writes configuration data to the underlying data store (etcd) and versions every stored system configuration. It is the backend to OMD Director, which is the Media Broadcaster configuration management GUI, and is responsible for serving the configuration data to the MCM.
- **Multicast Controller Manager (MCM):** The MCM polls the BCM at intervals to retrieve configuration data. It is the management component of an MC-Controller and controls the entire Cisco Media Broadcaster system. It also aggregates viewership data received by the SSR.
- **Data Store Service (etcd):** The etcd service stores all of the configuration data for the BCM.
- **Stream Status Receiver (SSR):** The SSR handles all of the incoming Stream Status messages and Config Requests from the MC-Receivers, also referred to as the Embedded Multicast Client (EMC). To handle the load of incoming Stream Status messages, there will be many instances of the SSR.

MC-Sender

The MC-Sender is an application that runs on a Linux operating system (bare metal, virtualized, or containerized) in the service provider premise. The primary functions of the MC-Sender are:

- Acquires a live ABR stream from the CDN or origin server using unicast HTTP/TCP requests and encapsulates the video data and FEC for multicast distribution.
- Transmits the data packets as a multicast stream to the multicast address group.
- Provides rate pace for the multicast video distribution rate.
- Can optionally provide QoS marking (DSCP) on the multicast data.

The MC-Sender contains the following subcomponents:

- **Multicast Server Interface (MSI):** Is the interface that the MC-Sender uses to communicate with the MC-Controller.
- **Multicast Sender Manager (MSM):** Creates, destroys, and configures individual MSA instances to convert a single ABR profile to a multicast stream.
- **Multicast Sender Application (MSA):** Acts as an HTTP client that pulls ABR content (manifests and segments) from the CDN and then sends out the segments using NAC Oriented Reliable Multicast (NORM) to all of the gateways. Each MSA delivers only one stream. Because each MC-Sender is capable of delivering many streams, an MC-Sender will have many MSAs.

MC-Receiver

The MC-Receiver, also referred to as the Embedded Multicast Client (EMC), is an application that can be integrated into the STB or home router that resides in the managed home of the service provider and runs in the CPE middleware operating system. The primary functions of the MC-Receiver are:

- Streams HTTP/TCP unicast video to HTTP ABR media player.
- Implements a proxy cache toward the HTTP media player.
- Acquires (ingests) ABR video using multicast or unicast, with transparent switching, and fills the proxy cache.
- Caches reliable fragmented HTTP video (HLS, DASH, and HSS)
- Provides packet error repair using in-band FEC when possible, and falls back to unicast HTTP retransmit from CDN.
- Streams to in-home multiple media player clients a common stream or multiple unique streams.

  The MC-Receiver intercepts ABR fragment requests from the end clients (iPads, iPhones, and STBs) and does one of the following:

- If the MC-Receiver has already received the requested content via multicast and still has it in its local cache, it will serve that content back to the end clients (iPads, iPhones, and STBs) without forwarding the request upstream to the CDN.

- If the MC-Receiver does not have a copy of the content in its cache, then it proxies the request upstream to be fulfilled by the CDN. When the response is returned from the CDN, the MC-Receiver will cache this content in its local cache so that it can provide the content for future requests from downstream clients for the same content.

The MC-Receiver consists of the following components:

- **Proxy Service:** Intercepts requests from downstream end user ABR clients and serves them using data from the local cache of the CPE (if available). If the content is not in the local cache of the CPE, the proxy requests the content from the CDN using unicast. The Proxy service will receive the configuration from the MC-Controller, which will determine which streams can be delivered using multicast. For any ABR client requests that can be delivered using multicast, the Proxy service will start a Multicast Receiver for that stream. When the ABR client stops watching the stream, the Proxy services will stop the Multicast Receiver for that stream. The Proxy Service can be thought of as part of the Control Plane.
- **Multicast Receiver:** The Multicast Receiver uses NORM with FEC to receive multicast content from the MC-Sender. After the content is received, the proxy service stores it in the local cache on the CPE. The MC Receiver will leave a multicast stream when no requests from any player has been received for certain amount of time. The Proxy service will determine when a Multicast Receiver needs to be started and stopped. The Multicast Receiver can be thought of as part of the Data Plane.

Channel Lineup

What content is delivered by the Cisco Media Broadcaster deployment is defined using a channel lineup. A channel lineup defines where to find the content, and what address and bit rate will be used for multicasting the content. The channel lineup is stored in the MC-Controller and is communicated to the MC-Sender via a StartMulticastReq message. When the MC-Sender receives a StartMulticastReq message, the MC-Sender sends an HTTP request for the manifest to the CDN. After receiving the manifest file, the MC-Sender starts to request the segments that are defined in the manifest and transmits them via reliable multicast (NORM) over the video network interface. MC-Sender continues the same operation of getting the latest manifest, requesting for segments based on the manifest and transmitting them via multicasting for a given video stream until the MC-Controller sends a StopMulticastReq message.

Channel lineups are configured in OMD Director and can also be imported into OMD Director using a CSV file. More channel lineup information can be found at Configuring Broadcasting Groups, on page 19 and Managing Broadcasting Groups, on page 33 within this guide.

Broadcasting Groups

A Broadcasting Group identifies which MC-Controllers and MC-Senders work together to provide multicasting services for a group of channels. All of the MC-Controllers and MC-Senders in a broadcasting group will use the same filtering rules and server specific settings. Broadcasting groups are part of the high availability (HA) solution of Media Broadcaster.

Media Broadcaster HA Architecture

Cisco Media Broadcaster provides a fully redundant solution for the MC-Controllers and MC-Senders. Media Broadcaster supports an Active/Standby HA solution for the MC-Controller components. For the MC-Senders,

all MC-Senders run simultaneously, but handle different multicast streams. If an MC-Sender becomes unavailable, all of the multicasting streams that were running on that MC-Sender are automatically redistributed to by the MC-Controller to the remaining MC-Senders based on the bandwidth usage of each MC-Sender.

MC-Controller HA Solution

Each MC-Controller consists a Broadcaster Configuration Manager (BCM), a Multicast Controller Manager (MCM), and many instances of Stream Status Receivers (SSRs). Cisco Media Broadcaster provides a fully redundant solution for each of these components.

HA for Broadcaster Configuration Manager

keepalived is installed on the BCM instances of all of the MC-Controllers in the Broadcasting group. keepalived, using Virtual Router Redundancy Protocol (VRRP), elects one of the BCM instances as the primary (master) and the remaining BCM instances will be standby (backup). The primary BCM and the standby BCMs use keepalived to communicate with each other to maintain an HA environment. If keepalived determines that the master (active) BCM instance is not available, it will elect a backup (standby) BCM instance as master.

A virtual IP address, also referred to as the floating IP address, is shared between the BCM instances in a Broadcasting group. This virtual IP address needs to be different for each Broadcasting group and must be different from the virtual IP address of any of the other MC-Controller components (such as MCM). keepalived will bind the floating IP address to the management interface of the BCM instance that is in the master state. The floating IP must be reachable by all the BCM instances in the Broadcasting group and must be on the same subnet as the IP addresses assigned to the management interface of the BCM instances.

The BCM instance that is the master will unicast VRRP messages to the backup BCMs. When there is an application or node failure of the master BCM, the VRRP advertisements will stop. The backup (standby) BCM instances will detect the absence of the VRRP messages and perform an election to choose a new master. Keepalived will then bind the floating IP address to the management interface of the new master BCM instance.

HA for Multicast Controller Manager

keepalived is installed on the MCM instances of all of the MC-Controllers in the Broadcasting group. keepalived, using Virtual Router Redundancy Protocol (VRRP), elects one of the MCM instances as the primary (master) and the remaining MCM instances will be standby (backup). The primary MCM and the standby MCMs use keepalived to communicate with each other to maintain an HA environment.

A virtual IP address, also referred to as the floating IP address, is shared between the MCM instances in a Broadcasting group. This virtual IP address needs to be different for each Broadcasting group and must be different from the virtual IP address of any of the other MC-Controller components (such as BCM). Keepalived will bind the floating IP address to the management interface of the MCM instance that is in the master state. The floating IP must be reachable by all the MCM instances in the Broadcasting group and must be on the same subnet as the IP addresses assigned to the management interface of the MCM instances.

keepalived monitors the master MCM by checking the response received from the master MCM health check API. If the response code from this health check API is not 200, keepalived signals that the master (active) MCM instance is not available and will elect a backup (standby) MCM instance as master. keepalived will then bind the floating IP address to the management interface of the new master MCM instance. The new master MCM will start the viewership monitoring cycle so that the new master MCM can start collecting viewership data and manage dynamic channels after one monitoring period has passed.

The active MCM will always point to the floating IP address of the BCM. This makes sure that if the active BCM instance goes down, the active MCM will keep receiving configuration data because keepalived will automatically select a new BCM instance from the backup instances.

HA for Stream Status Receiver

SSR is a service that handles the Stream Status and Config Request messages from the MC-Receivers. To handle the load of incoming Stream Status messages, there will be many instances of the SSR running on one MC-Controller. httpd distributes the incoming Stream Status and Config Request messages to the SSR instances to process.

In a Media Broadcaster HA deployment, HAProxy is used to load balance the Stream Status and Config Request messages that come from the MC-Receivers to the SSRs, through httpd, that are running on all of the MC-Controllers in the Broadcasting group. An HAProxy instance running keepalived will run on each MC-Controller in the Broadcasting group. keepalived, using Virtual Router Redundancy Protocol (VRRP), will elect one of the HAProxy instances as the primary (master) and the remaining HAProxy instances will be standby (backup). The primary HAProxy and the standby HAProxies use keepalived to communicate with each other to maintain an HA environment.

A virtual IP address, also referred to as the floating IP address, is shared between the HAProxy instances in a Broadcasting group. This virtual IP address needs to be different for each Broadcasting group and must be different from the virtual IP address of any of the other MC-Controller components (such as MCM). keepalived will bind the floating IP address to the video interface of the HAProxy instance that is in the master state. The floating IP must be reachable by all the HAProxy instances in the Broadcasting group and must be on the same subnet as the IP addresses assigned to the video interface of the HAProxy instances. Because the messages from the MC-Receivers come from the public Internet, the floating IP address for the HAProxy service must be accessible from the public Internet.

The HAProxy instance that is the master will unicast VRRP messages to the backup HAProxies. When there is an application or node failure of the master HAProxy, the VRRP advertisements will stop. The backup (standby) HAProxy instances will detect the absence of the VRRP messages and perform an election to choose a new master. keepalived will then bind the floating IP address to the video interface of the new master HAProxy instance.

The MC-Receivers will send the Stream Status and Config Request messages to the virtual (floating) IP address that is assigned to the HAProxy instance.

MC-Sender HA Solution

The goal of HA for the MC-Senders is to provide high availability for the multicasting streams that are being serviced by the MC-Senders. All MC-Senders in a Broadcasting group run simultaneously, but handle different multicast streams. If an MC-Sender becomes unavailable, all of the multicasting streams that were running on that MC-Sender are automatically redistributed by the active MCM to the remaining MC-Senders based on the implemented policy. The current policy is based on the bandwidth usage of each MC-Sender, and the multicasting stream will be assigned to the MC-Sender with the lowest bandwidth usage.

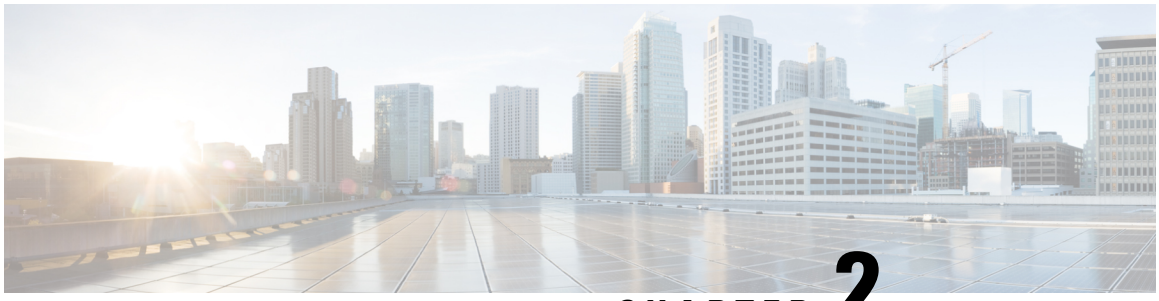
When the channel lineup is created, it will be assigned a unique source IP address that is used regardless of which MC-Sender will multicast the stream for this channel. This means that if the MC-Sender that is streaming the channel changes, it is transparent to the MC-Receivers. When an MC-Sender is assigned a channel by the MCM and beings multicasting the stream, the MC-Sender adds the source address for that channel to the interface for multicasting network (video interface). The MC-Sender uses OSPF to advertise this source address to the routers in the Multicast core and access network. When the MC-Sender stops multicasting the stream for the channel, it removes the source address from the interface and OSPF will stop advertising this address.

Cisco OMD Director

Cisco Open Media Distribution (OMD) Director is a cloud-based element management system that provides provisioning, monitoring and role-based management for Cisco Media Broadcaster. OMD Director is a common management system for both Cisco Media Broadcaster and Cisco Media Streamer (the Cisco unicast CDN solution). When Cisco Media Streamer is deployed with the Cisco Media Broadcaster solution, a common OMD Director instance is used to provision, monitor, and analyze both the unicast CDN of Media Steamer and the distribution of multicast streams by Media Broadcaster.

Cisco OMD Director is the primary user interface for the Cisco Media Broadcaster solution. It provides a unified interface to seamlessly manage the different components of the Media Broadcaster platform. OMD Director enables the administrator to rapidly configure Broadcasting Groups, including channel lineups and filtering rules, and integrates monitoring into a single management tool.

Cisco OMD Director is implemented to be virtualized and further optimized with microservices in containers. Microservices provide modularity between components of the system enabling individual microservices to be replaced, upgraded or scaled up independently of one another. Microservices never share data directly via a database, only through their external APIs and each microservice is responsible for maintaining its own data store.



CHAPTER 2

Cisco OMD Director Overview

Cisco OMD Director is the primary user interface for Cisco Media Broadcaster and Cisco Media Streamer. It provides a unified interface to seamlessly manage the different components of the Cisco OMD deployment. OMD Director enables the administrator to easily provision broadcasting groups and channel lists.

This chapter describes how to log in to Cisco OMD Director, provides a high-level overview of the product, and describes the menu options that will be used to manage Media Broadcaster. Some of the OMD Director menus apply only to Media Streamer functions. This guide will not cover those menus. For more information on managing a Media Streamer deployment, see the Cisco Media Streamer User Guide.

This chapter includes the following sections:

- Accessing OMD Director, on page 9
- OMD Director User Interface Elements, on page 11
- OMD Director Navigation Panel: Monitor Overview, on page 13
- OMD Director Navigation Panel: Administration, on page 14
- OMD Director Navigation Panel: Support, on page 14
- OMD Director Navigation Panel: Media Broadcaster > Broadcasting Groups, on page 17
- OMD Director Navigation Panel: Media Broadcaster > Insights, on page 18

Accessing OMD Director

The following sections describe how to access the OMD Director GUI. To access the OMD Director GUI, you must be using one of the following supported browsers:

- Firefox version 59 or later
- Chrome version 66 or later

OMD Director HA

OMD Director supports an Active/Standby High Availability (HA) configuration and supports inter-site redundancy. OMD Director HA provides the following:

- Prevents the loss of any configuration data due to a hardware, software, or network failure
- Minimizes the loss of monitoring data such as time series metrics, alarms, and notifications due to a hardware, software, or network failure

- Makes sure alarm emails continue to be sent
- Continues to support streaming capabilities

In an OMD Director HA configuration, your OMD Director instance can be running in either primary or backup mode. If either the OMD Director primary or backup instance loses connection or fails, the remaining OMD Director instances will transition into a detached state.

The following describes the actions you can perform depending on the mode of the OMD Director instance that you are logged into:

- **Primary:** You can only make configuration changes from the primary OMD Director instance. The primary instance is the authoritative instance for all data. Changes to all configurations made from the primary OMD Director instance are replicated to the backup instance.
- **Backup:** While logged into the OMD Director instance that is running in backup mode, you can only view the configuration, you cannot make any changes to the configuration. Any buttons or links that would allow configuration changes will be disabled on the backup OMD Director instance. If you are logged into the backup OMD Director instance, the title bar will show "This OMD Director is currently running in backup mode".
- **Detached:** While an OMD Director instance is running in a detached state, you can view the configuration and you can acknowledge, clear, and comment on alarms. The buttons or links for any actions that are not allowed will be disabled. If you are logged into an OMD Director instance that is running in the detached state, the title bar will show "This OMD Director is currently running in detached mode".

If the primary OMD Director instance fails, you must manually configure the backup OMD Director instance as the new primary OMD Director instance. For more information on this procedure, see the *Cisco Media Streamer and Cisco Media Broadcaster Installation and Upgrade Guide*.

Log in to OMD Director

Follow these steps to log in to OMD Director:

Before you begin

If you are running OMD Director in an HA configuration, make sure you are logging into the OMD Director Primary instance if you want to make changes to the CDN configuration.

Note If needed, OMD Director can be configured to only display Media Broadcaster menus, without the Media Streamer options. In that case, menu items will consist of Media Broadcaster, Monitor, Administration, and Support. For details on configuring your OMD Director user interface to be Media Broadcaster centric, see the *Cisco Media Streamer and Cisco Media Broadcaster Installation and Upgrade Guide*.

Procedure

Step 1 From a web browser, use HTTPS and enter the hostname or IP address of OMD Director and port number 8099. For example:

```
https://<omd_director_worker_hostname_or_ip_address>:8099
```

The OMD Director login page is displayed.

Step 2 Log in with your username and passphrase. If this is the first time you are logging in, enter the username and passphrase that was emailed to you by the system. You will be prompted to change your passphrase as part of your first login.

Note Only users with the role of Administrator will be able to access the Media Broadcaster menus.

Step 3 After you log in, the OMD Director home page appears. The home page is the CDN Edge monitor page. If you are logged into either an OMD Director node running in standalone mode or the primary OMD Director node in an HA installation, the title bar of the window should be solid and there will be no message showing the state.

Note If you are running an instance of OMD Director that is supporting only a Media Broadcaster deployment and not a Media Streamer deployment, the charts will indicate that there is no data to display.

If you are logged into the Backup OMD Director instance, the title bar of the window will show "This OMD Director is currently running in backup mode".

If you are logged into an OMD Director instance that is running in the detached state, the title bar of the window will show "This OMD Director is currently running in detached mode".

Note Each user can only have one active login at a time. If a user logs in with the same username from another system or browser, they will be prompted to either force the login, which will log off the current user session, or cancel the log in and log in as another user.

Logging Out of OMD Director

To log out of OMD Director:

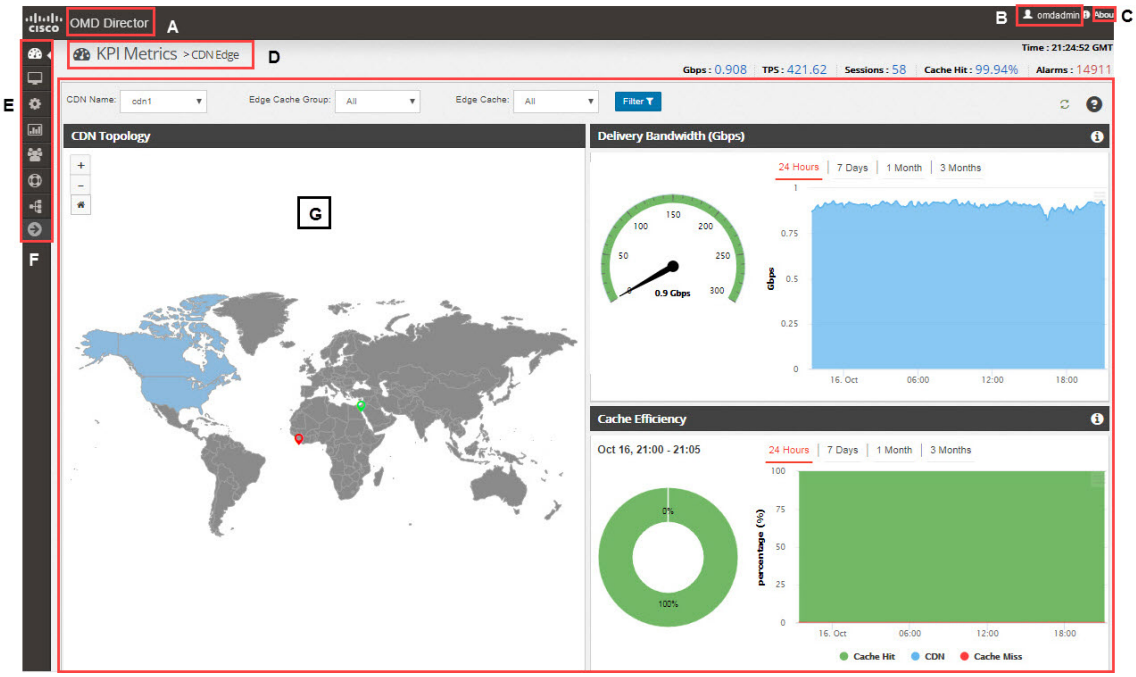
Procedure

Step 1 Click your username in the upper-right corner of the window.

Step 2 Choose the **Logout** option.

OMD Director User Interface Elements

The following describes the elements within the OMD Director UI:



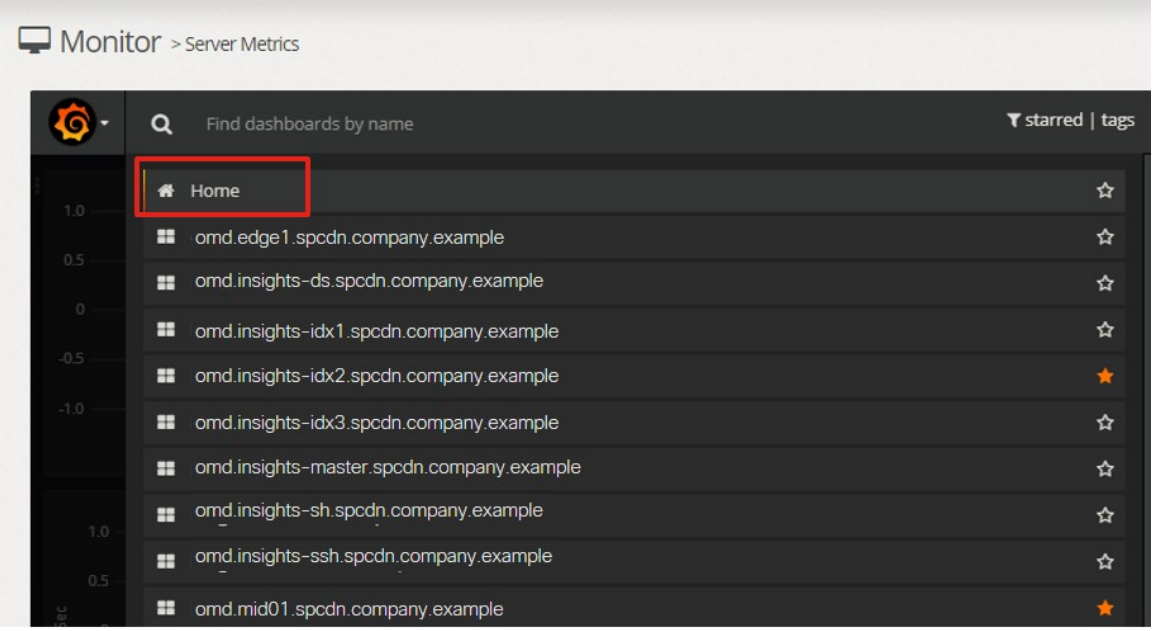
- **(A) Product Name:** Displays the name of the product (OMD Director).
- **(B) User:** Displays the user name of the currently logged in user. From this element you can logout and you can change profile settings of the current user, including the passphrase.
- **(C) About:** Clicking the about link displays the current versions of the OMD Director components. This can be helpful when reporting issues or troubleshooting problems with OMD Director.
- **(D) Current Page:** Displays the path of the current page.
- **(E) Navigation Panel:** Provides the menus to navigate to the different functions of OMD Director. The navigation panel contains the following choices:
  - KPI Metrics
  - Monitor
  - Provisioning
  - Insights
  - Administration
  - Support
  - Media Broadcaster
- **(F) Expand Menu:** Click this icon to expand the navigation panel and display it in a menu structure. To minimize the navigation panel back to icons only, click the right arrow icon that appears.
- **(G) Main Area:** The information that is displayed in this area depends on what menu you choose.

OMD Director Navigation Panel: Monitor Overview

From the Monitor menu you can view Media Broadcaster server metrics and alarms. This section will provide an overview of the options available from this menu that pertain to Media Broadcaster. For more detailed information on each option, see Media Broadcaster Monitoring, on page 49.

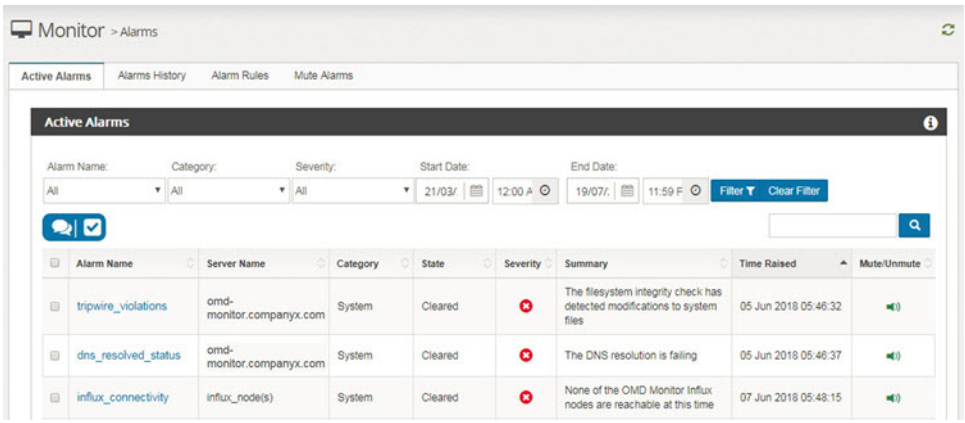
Monitor > Server Metrics

The **Monitor > Server Metrics** menu option launches a page that enables you to see a list of all of the physical and virtual servers used by OMD. From this list you can choose a server that will then display detailed historical server metrics about this server such as CPU utilization, Memory Utilization, Disk I/O, and other lower level server data.



Monitor > Alarms

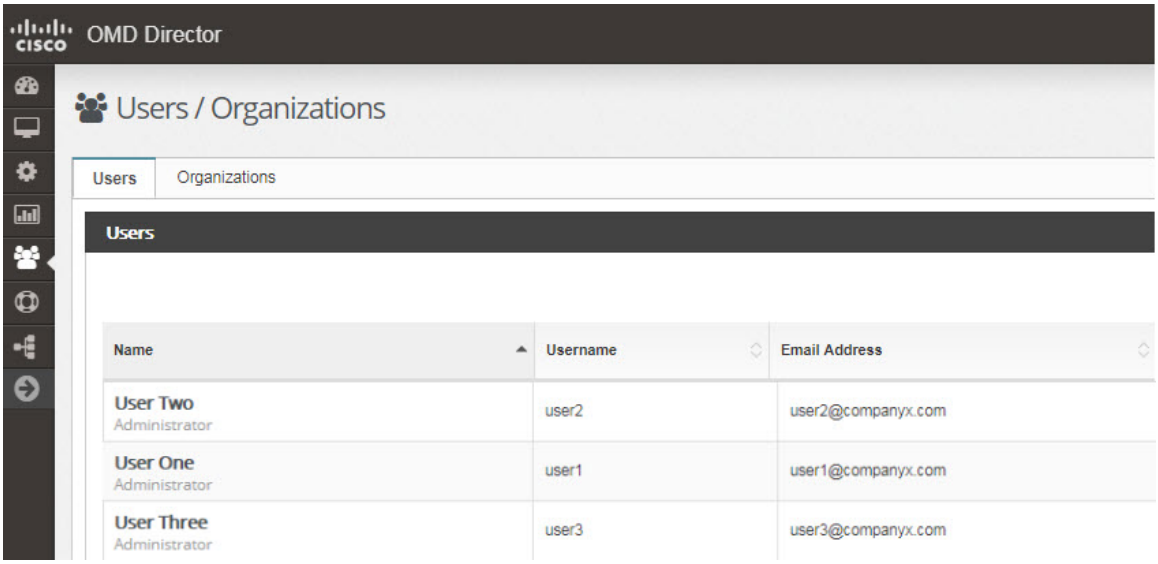
The **Monitor > Alarms** menu option displays the OMD system alarms that have been raised in the Media Broadcaster and Media Streamer environment, based on thresholds that are set. From the **Monitor > Alarms** page you can also view alarms, configure thresholds for the alarms, and mute alarms.



OMD Director Navigation Panel: Administration

The Administration menu enables you to see and manage the users who have access to OMD Director, including their privileges in the system. From the Administration menu you can also manage the backups of the OMD databases, including adding remote backup destination. The Administration menu also enables you to display an activity log that shows both user authentication and authorization activity, and configuration activity.

For more information on managing the OMD Director users, see OMD Director Administration, on page 71.



OMD Director Navigation Panel: Support

The Support menu provides the following information:

- **OMD Well Known Ports:** Displays information intended for the security personnel of an organization about the ports and protocols that need to be open between devices in the environment and other systems.
- **Contact:** Provides contact information for Cisco support.

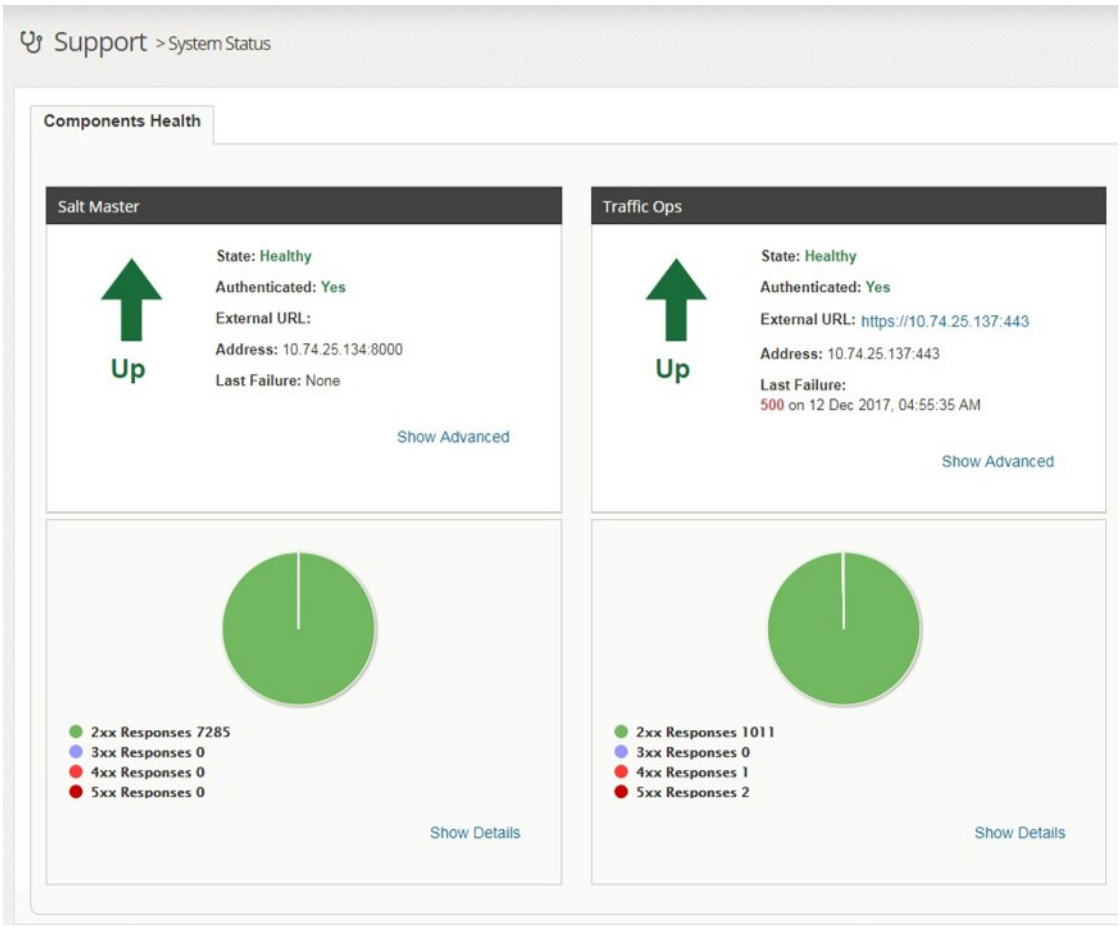
- **System Status:** Displays information about the connection to the Salt Master server and the Traffic Ops server, and a historical count of the different HTTP response codes that have been received by the servers since the CDN Manager microservice was started.

  Note The Traffic Ops server is used in a Media Streamer deployment.

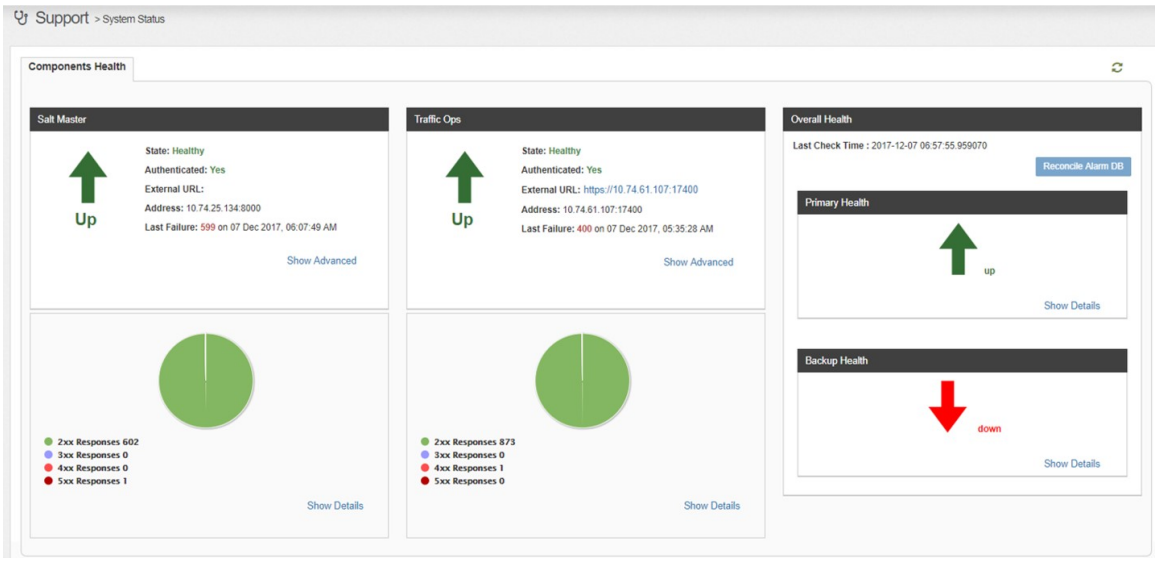
  When you choose **Support > System Status**, the Components Health tab is displayed. This tab displays the following information for both the Salt Master and Traffic Ops servers:

  - **State:** The State will be either Healthy or Unhealthy. This state is based on an overall summary of the connection to the server based on a combination of the authentication status, last response code, and recent response history.
  - **Authenticated:** This field is True if the username and passphrase that was configured can connect to server. Otherwise this field will display False.
  - **External URL:** Displays the address that cache servers can use to connect to the server. This address is often the public IP address of a NAT configuration or an Openstack Floating IP address.
  - **Address:** Displays the Hostname or IP address, and port number that was configured for the server.
  - **Last Failure:** Displays the HTTP Status Response code and timestamp of the last error on the server.
  - **Show Advanced:** When you click Show Advanced, the contents of the JSON file is displayed. This JSON file is used to determine the values of the information that is displayed for the servers on the Components Health tab.
  - **Response Code Table and Pie Chart:** Display a historical count of the different HTTP response codes that the server has received since the CDN Manager microservice was started.

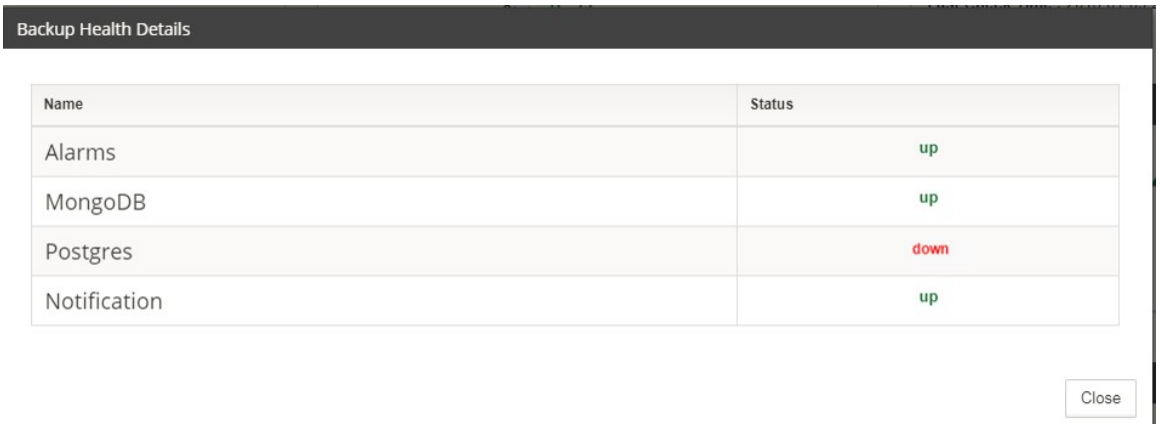


To refresh the information on the Components Health tab, click the **Refresh** button, located at the upper-right corner of the page.

If you are running OMD Director in a HA configuration, the Components Health window will also show the overall health of the Primary and Backup OMD Director instances. The following is an example:



To check the status of the individual services that run on either the Primary or the Backup, click the **Show Details** link. The following is an example:



OMD Director Navigation Panel: Media Broadcaster > Broadcasting Groups

The **Media Broadcaster > Broadcasting Groups** menu enables you to manage the Media Broadcaster broadcasting groups. From the **Media Broadcaster > Broadcasting Groups** menu you can:

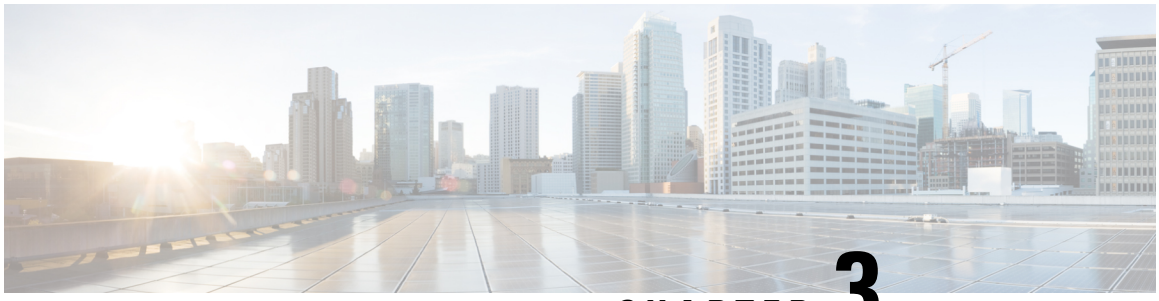
- View the MC-Controllers and MC-Senders that are part of the broadcasting group.
- View, create, and edit the channel lineup of a group.
- View, create, and edit the filtering rules for the broadcasting group
- View and edit the advanced Multicast Controller, Multicast Sender, and Multicast Receiver (Embedded Multicast Client) settings.

Refer to Configuring Broadcasting Groups, on page 19 and Managing Broadcasting Groups, on page 33 for details on how to configure and manage Media Broadcaster broadcasting groups.

OMD Director Navigation Panel: Media Broadcaster > Insights

Choosing the **Media Broadcaster > Insights** menu from the navigation panel launches OMD Insights, powered by Splunk for big data analysis. This page provides deep analytics of the Media Broadcaster environment that is based on mining data from logs located on the MC-Controllers and MC-Senders. This enables OMD Insights to provide comprehensive Media Broadcaster operational analytics, including analysis of fetch times, network utilization, and the efficiency of multicast content delivery.

Note For detailed information on the reports available from the Media Broadcaster > Insights menu, see Media Broadcaster Insights, on page 65.



CHAPTER 3

Configuring Broadcasting Groups

After you have installed Cisco Media Broadcaster, you need to configure the broadcasting groups in OMD Director. A broadcasting group identifies which Multicast Controllers and Multicast Senders work together to provide multicasting services for a group of channels and defines the settings for the Multicast Controllers and Multicast Senders that are part of that group.

To configure the broadcasting groups in Media Broadcaster, you will need to do the following within OMD Director:

- Add the broadcasting group to OMD Director
- Define the channel lineup
- Configure the filtering rules
- Configure the Multicast Controller settings
- Configure the Multicast Sender settings
- Configure the Embedded Multicast Client settings

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this chapter, make sure you are logging into the Primary OMD Director instance. If you are logged into an OMD Director instance that is running in Backup mode, the header of the window will show "This OMD Director is currently running in backup mode". If you are logged into an OMD Director running in a detached state because of an HA failure, the header will show "This OMD Director is currently running in detached mode".

This chapter includes the following sections:

- Add a Broadcasting Group, on page 19
- Configure a Broadcasting Group, on page 22

Add a Broadcasting Group

To be able to use OMD Director to manage the broadcasting groups of Media Broadcaster, you must first add the broadcasting group to OMD Director. Perform the following steps to add a Media Broadcaster broadcasting group to OMD Director:

Procedure

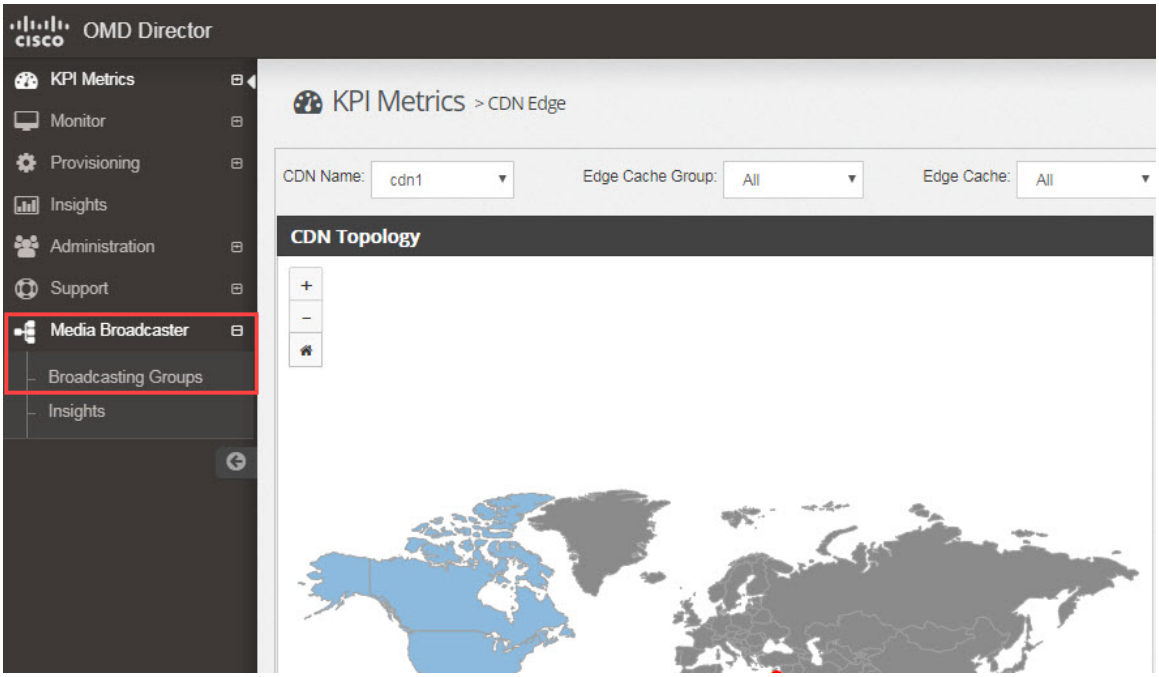
Step 1 Log in to the OMD Director GUI:

`https://<omd_director_worker_hostname_or_ip_address>:8099`

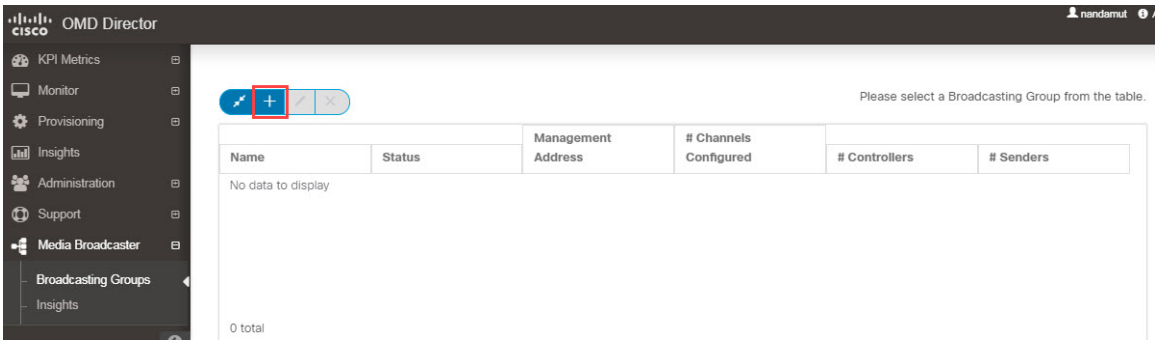
Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this section, make sure you are logging into the Primary OMD Director instance.

Step 2 Log in with your username and passphrase. If this is the first time you are logging in, enter the username and passphrase that was emailed to you by the system. You will be prompted to change your passphrase as part of your first login.

Step 3 Choose **Media Broadcaster > Broadcasting Groups**.



Step 4 From the window that appears, at the top of the window click the **Add** (+) button to add an existing broadcasting group to OMD Director. The broadcasting groups are created as part of the Media Broadcaster installation. For more information on installing Media Broadcaster, please see the *Cisco Media Streamer and Cisco Media Broadcaster Installation and Upgrade Guide*.



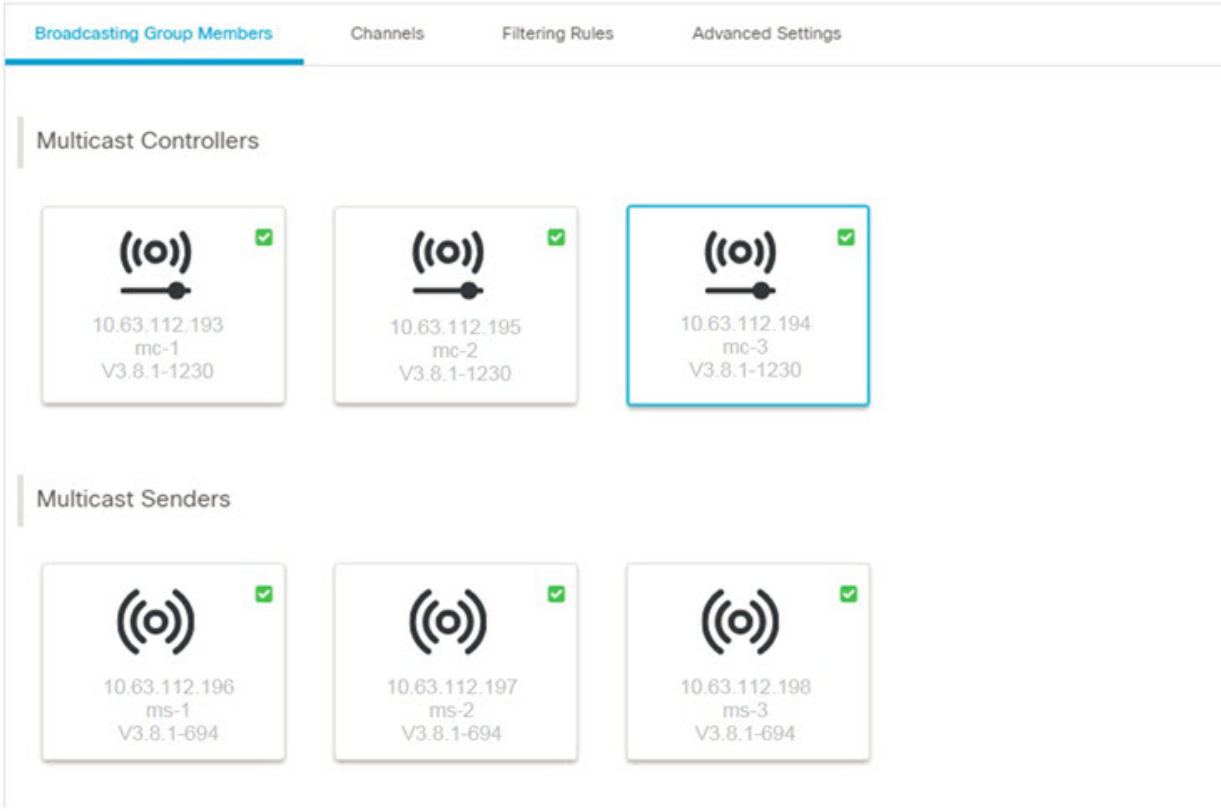
Step 5 In the Add Broadcasting Group window that appears, configure the following fields:

- **Name:** Enter a descriptive name for the broadcasting group.
- **Broadcasting Group Address:** If Media Broadcaster is deployed in a HA configuration, enter the floating IP address of the Broadcaster Configuration Manager (BCM) for this group that was configured when Media Broadcaster was installed. If Media Broadcaster is not deployed in an HA configuration and there is only one Multicast Controller for the broadcasting group, enter the IP address of that BCM.
- **Broadcasting Group Port:** Enter the port number that the OMD Director needs to use to communicate with the BCM. This is based on the configuration of the BCM. If the BCM is configured to use HTTPS, enter 443. If the BCM is configured to use HTTP, enter 80.

Step 6 When you are finished entering the values for the broadcasting group, click **Save**.

Step 7 After you add the group, OMD Director will retrieve the information for the Multicast Controllers and Multicast Senders in that group and display them on the **Broadcasting Group Members** tab. The following information will be shown for each Multicast Controller and Multicast Sender that is part of the group:

- IP address
- Hostname
- Media Broadcaster software version
- Status of the server
  - A check mark in the upper-right hand corner of the server icon means the server is available. A dash in the upper-right hand corner of the server icon means the server is unavailable.
- The Multicast Controller that is highlighted with a blue box is the active Multicast Controller. In the following example, mc-3 is the active Multicast Controller.



Configure a Broadcasting Group

After you add a broadcasting group, you need to configure that broadcasting group. Configuring the broadcasting group includes:

- Defining the channel lineup
- Configuring the filtering rules
- Configuring the Multicast Controller settings
- Configuring the Multicast Sender settings
- Configuring the Multicast Receiver settings

You can use the Edit Broadcasting Group wizard to configure the broadcasting group.

Define the Channel Lineup

The channel lineup defines what content Media Broadcaster should multicast and the source of that content. The channel lineup also defines what multicast address to use to multicast the content, the type of content

(audio or video), and the format of the media. Perform the following steps to define the channel lineup for the broadcasting group:

Procedure

Step 1 The most efficient way to add channels to the channel lineup is to import a CSV file that contains the channel information. From a system that has access to the OMD Director GUI, refer to the Channel Lineup CSV File Structure table to create a CSV file that has the required fields to import channels to the broadcasting group.

Table 1: Channel Lineup CSV File Structure

Field	Definition

channelId	Name of the channel. The channel ID is contained in the requested segment URL. This value is used to identify requests from the media player in a managed home that are candidates for multicasting. Each channel ID can have only one audio and one video entry in the channel lineup.
	For example, in the following segment URL, `live66.3-wutf` is the Channel ID:
	`http://edgec99.live.companyx.com/Apple/live`
	`/live66.3-wutf/StreamA-2095000`
	`/Seg_12078/StreamA-2095000_1207812.ts`

masterManifestUrl	The URL of the top level manifest for the linear asset.
multicastAddress	The multicast address to use when multicasting this linear asset.
multicastPort	The port number to use when multicasting this linear asset.
sourceAddress	The IP address the Multicast Sender will use as the source address when multicasting the linear asset. • If there is only one Multicast Sender in the Media Broadcaster deployment, you can use the IP address assigned to the video interface of the Multicast Sender as the source address. • If there are multiple Multicast Senders in the Media Broadcaster deployment, you must use dynamic routing and enter a unique source address that is on the OSPF network for each channel.

Field	Definition
multicastMode	The mutlicastMode can be either static or dynamic: • **static:** The Multicast Controller will tell the Multicast Sender to start multicasting the linear asset whenever the channel lineup is defined. • **dynamic:** The Multicast Controller will tell the Multicast Sender to start multicasting the linear asset when the Multicasting Start Threshold has been met. The Multicasting Start Threshold defines how many viewers must be watching a particular stream before the multicast service for that stream is started. **Note** The Multicasting Start Threshold is configured on the **Advanced Settings** tab of the Edit Broadcasting Group wizard.
senderMode	This field can be one of these options as chosen in the Director user interface: • **Segment:** When the Sender mode is set to "Segment" for the channel, the MC-Sender waits to multicast the segment to the clients until the entire segment has been received from the Origin Server. • **Chunked:** When the Sender mode is set to "Chunked" for the channel, this indicates that the MC-Sender is receiving the segments from the Origin Server in segment slices, referred to as "chunks". The MC-Sender will begin multicasting these chunks to the clients as soon a complete chunk is received from the Origin Server; the MC-Sender does not have to wait for all of the segment chunks to be received from the Origin Server before it can begin multicasting chunks to the clients.
mediaFormat	ABR format for this linear asset. This can be HLS, DASH, or HSS.
mediaType	Media type for this linear asset. This can be either Audio or Video.

Field	Definition

repId	Representation Identifier for this linear asset.
	Instead of including the bit rate for the encoding itself in the URL, it is possible that a representation identifier is used instead. It is also possible that the repId will be the same as the bitrate.
	The Representation ID is part of the segment URL. For example, in the following segment URL, 2095000 is the Representation Identifier.
	`http://edgec99.live.companyx.com/Apple/live/live66.3-wutf`
	`/StreamA-2095000/Seg_12078/StreamA-2095000_1207812.ts`

bitrate	Bit rate of the linear asset.

The following is an example of a CSV file that could be used to import a channel lineup:

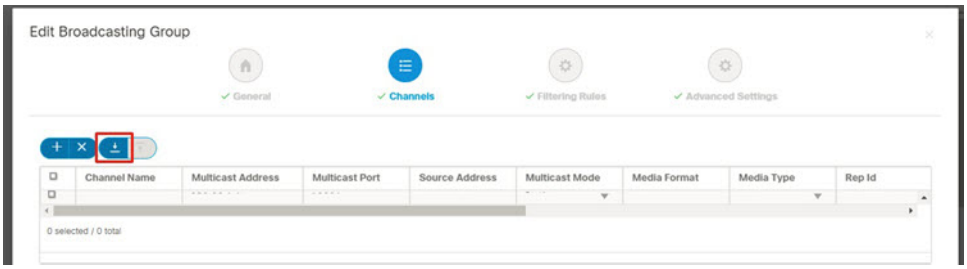
```
channelId,masterManifestUrl,multicastAddress,multicastPort,sourceAddress,multicastMode,senderMode,mediaFormat,mediaType,
repId,bitrate
live66.1-wutf,http://edgec99.live.cdn.companyx.com/Apple/live/live66.1-wutf/StreamG-112000.m3u8,
236.66.1.2,10002,198.51.100.2,Static,Chunked,HLS,Audio,112000,196000
live66.2-wutf,http://edgec99.live.cdn.companyx.com/Apple/live/live66.2-wutf.m3u8#bandwidth=2095000,
236.66.2.1,10003,198.51.100.3,Static,Chunked,HLS,Video,2095000,2095000
live66.2-wutf,http://edgec99.live.cdn.companyx.com/Apple/live/live66.2-wutf/StreamE-112000.m3u8,
236.66.2.2,10004,198.51.100.4,Static,Segment,HLS,Audio,112000,196000
live66.3-wutf,http://edgec99.live.cdn.companyx.com/Apple/live/live66.3-wutf.m3u8#bandwidth=2095000,
236.66.3.1,10005,198.51.100.5,Static,Segment,HLS,Video,2095000,2095000
live66.3-wutf,http://edgec99.live.cdn.companyx.com/Apple/live/live66.3-wutf/StreamE-112000.m3u8,
236.66.3.2,10006,198.51.100.6, Static,Segment,HLS,Audio,112000,196000
live66.4-wutf,http://edgec99.live.cdn.companyx.com/Apple/live/live66.4-wutf.m3u8#bandwidth=2095000,
236.66.4.1,10007,198.51.100.7,Static,Segment,HLS,Video,2095000,2095000
live66.4-wutf,http://edgec99.live.cdn.companyx.com/Apple/live/live66.4-wutf/StreamE-112000.m3u8,
236.66.4.2,10008,198.51.100.8,Static,Segment,HLS,Audio,112000,196000
live66.4-wutf,http://edgec99.live.cdn.companyx.com/Apple/live/live66.4-wutf/StreamE-112000.m3u8,
236.66.4.3,10008,198.51.100.8,Static,Segment,HLS,Video,196000,196000
```

Note Make sure the CSV file does not have a new line entry at end of the file or this will cause a validation error when importing the file.

Step 2 Choose **Media Broadcaster > Broadcasting Groups**. From the list of broadcasting groups, choose the group you want to edit and click the Edit icon above the list. The Edit Broadcasting Group wizard appears.

Step 3 From the Edit Broadcasting Group wizard, from the General step click **Next** to go to the Channels list or click the **Channels** icon at the top.

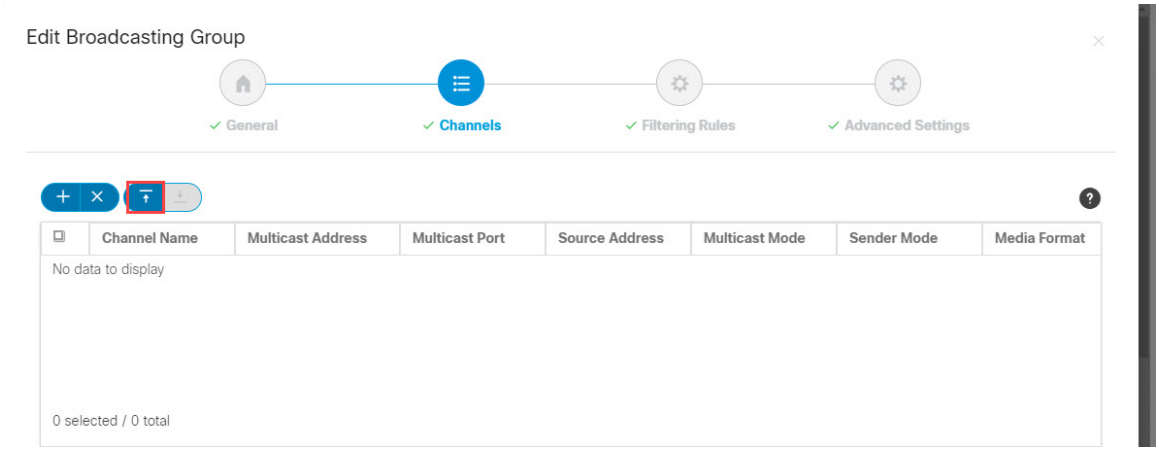
Step 4 After you have created the channel lineup CSV file, from the **Channels** tab in the Edit Broadcasting Group wizard click the **Import Channels** icon.



Step 5 From the Import Channels pop-up window, click **Choose File** and browse for the CSV file that you created in Step 1. When you choose the file, OMD Director will verify that it can parse the file correctly.

Step 6 If the CSV file is parsed correctly, the **Import** button will be enabled. Click the **Import** button to import the channel lineup.

Warning When you click **Import**, the channel importer will replace all the existing channels in the list.



Step 7 To add a single channel to the lineup, click the **Add** (+) icon. A new row will appear at the bottom of the list. Enter the following information for the new channel:

- **Channel Name:** Name of the channel. The channel ID is contained in the requested segment URL. This value is used to identify requests from the media player in a managed home that are candidates for multicasting. Each channel ID can have only one audio and one video entry in the channel lineup.
- **Multicast Address:** The multicast address to use when multicasting this linear asset.
- **Multicast Port:** The port number to use when multicasting this linear asset.
- **Source Address:** The IP address the Multicast Sender will use as the source address when multicasting the linear asset.
- **Multicast Mode:** Choose the static or dynamic multicast mode:
  - **static:** The Multicast Controller will tell the Multicast Sender to start multicasting the linear asset at startup.
  - **dynamic:** The Multicast Controller will tell the Multicast Sender to start multicasting the linear asset when the Multicasting Start Threshold has been met. The Multicasting Start Threshold defines how many viewers must be watching a particular stream before the multicast service for that stream is started.

Note The Multicasting Start Threshold is configured on the **Advanced Settings** tab of the Edit Broadcasting Group wizard.

- **senderMode:** Chooses between the following sender modes:
  - **Segment:** When the Sender mode is set to "Segment" for the channel, the MC-Sender waits to multicast the segment to the clients until the entire segment has been received from the Origin Server.
  - **Chunked:** When the Sender mode is set to "Chunked" for the channel, this indicates that the MC-Sender is receiving the segments from the Origin Server in segment slices, referred to as "chunks". The MC-Sender will begin multicasting these chunks to the clients as soon a complete chunk is received from the Origin Server; the MC-Sender does not have to wait for all of the segment chunks to be received from the Origin Server before it can begin multicasting chunks to the clients.
- **Media Format:** Enter the media format of the channel. This can be HLS, DASH, or HSS.
- **Media Type:** Choose either Audio or Video.
- **Rep Id:** Representation Identifier for this linear asset. The Representation ID is part of the segment URL.
- **Bitrate:** Bitrate of the channel.
- **Master Manifest URL:** The URL of the top level manifest for the linear asset.

Step 8 After the channels have finished importing, they will appear in the Channels list. Click **Next** or click the **Filtering Rules** icon at the top of the window to go to the next step, configuring the filtering rules.

Configure the Filtering Rules

The MC-Receiver uses the information configured on the Filtering Rules tab to identify which requests made by an HTTP media player are relevant to multicasting. The entries in the Allowed Servers field determine on which URLs requested by the media player the MC-Receiver should be further processed using REGEX match.

After the MC-Receiver determines that the URL requested by the media player should be checked for a REGEX match, PERL Compatible Regular Expressions (PCRE) uses the regular expressions configured in the Multicast URL Regex field to determine whether or not the stream being requested by the media player is available via multicast. The domain, content identifier, and bit rate of the URL requested by the media player are compared to the regular expressions configured in the Multicast URL Regex field. If there is a match against one of the configured regular expressions, the content identifier and bit rate portions of the URL are then compared against the same fields in the channel lineup of the broadcasting group. If a match is found, the MC-Receiver will join the multicasting group for that channel.

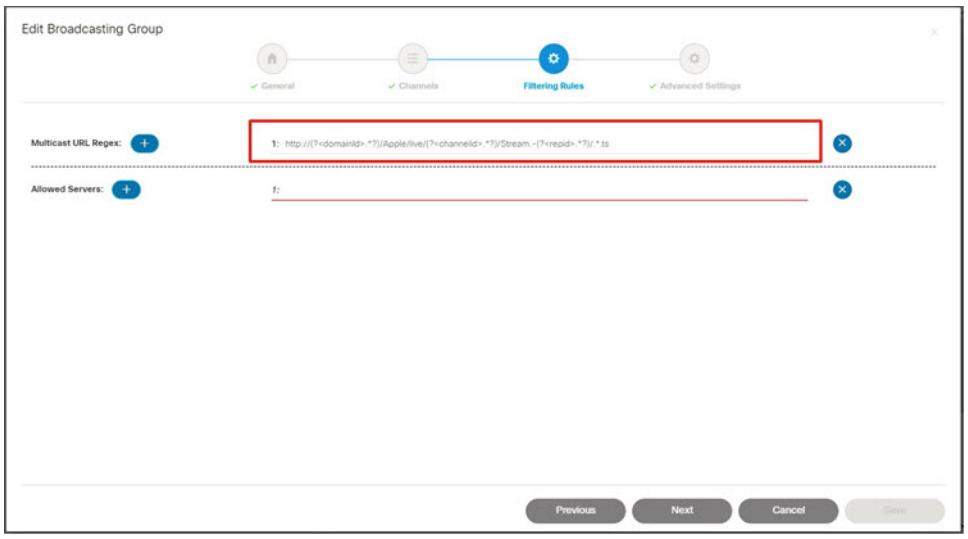
Perform the following steps to configure the Filtering Rules for the broadcasting group:

Procedure

Step 1 In the Multicast URL Regex field on the Filtering Rules tab, enter a regular expression to identify which requests made by a managed home media player are relevant to multicasting. For example:

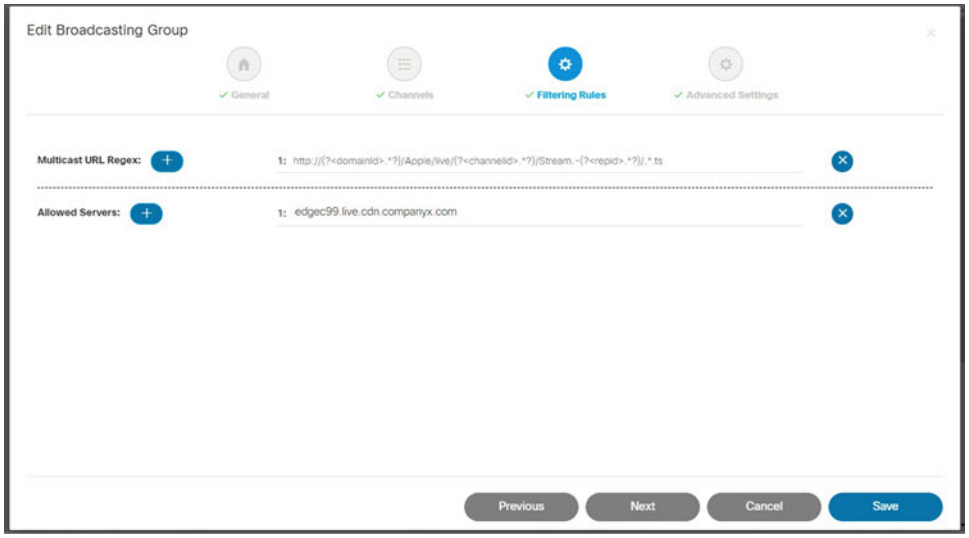
```
http://(?<domainId>.*?)/Apple/live_stream/(?<channelid>.*?)/Stream.-(?<repid>.*?)/.*.ts.
```

This example uses capturing groups to extract the domain, channel ID, and Representation ID from the URL for comparison against the channel lineup.



Step 2 At times, you will find that more than one regular expression is needed. For example, during a transition period from one URL format to another, it might be necessary to have the MC-Receiver support both the "old" URL style and the "new" URL style as content migrates from one system to the other. Therefore, you can configure more than one Multicast URL Regex. To enter an additional Multicast URL Regex value, click the **Add** (+) icon next to Multicast URL Regex. To remove a Multicast URL Regex entry, click the **Delete** (x) icon at the end of the row for the Multicast URL Regex you want to delete.

Step 3 In the **Allowed Servers** field, enter an FQDN or IP address for which the MC-Receiver should perform HTTP GET processing on to determine REGEX matches. If you need to enter more than one FQDN or IP address, click the **Add** (+) icon next to Allowed Servers. To remove an Allowed Servers entry, click the **Delete** (x) icon at the end of the row for the Server you want to delete.



Step 4 When you are finished adding the Multicast URL Regex expressions and the allowed servers, click **Next** or click the **Advanced Settings** icon at the top of the window to go to the next step, configuring the advanced settings.

Configure Advanced Settings

The advanced settings of the broadcasting group define settings for the Multicast Controllers, Multicast Senders, and Embedded Multicast Clients (also referred to as the MC-Receiver) of the group. All Multicast Controllers, Multicast Senders, and MC-Receivers in the group will use the same settings.

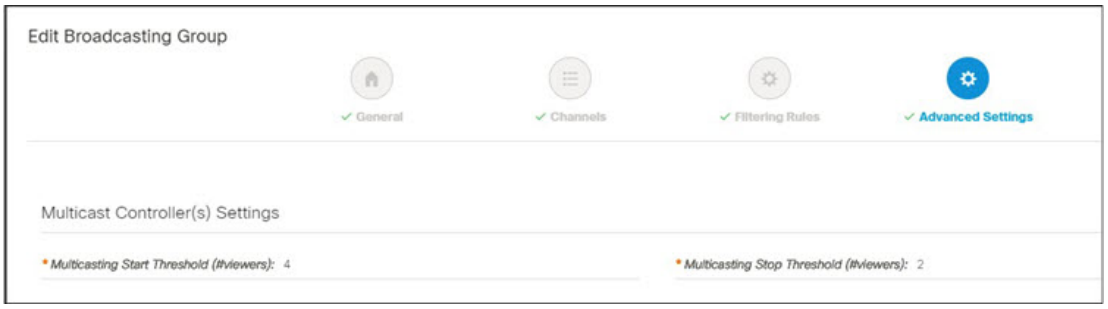
Perform the following steps to configure the advanced settings of the Multicast Controllers, Multicast Senders, and Embedded Multicast Clients (MC-Receivers):

Procedure

Step 1 On the **Advanced Settings** tab, edit the following fields to configure the Multicast Controller settings of the broadcasting group:

- **Multicasting Start Threshold (#viewers):** For a channel that is configured with a Multicast Mode of dynamic, enter the minimum number of viewers that must be watching that stream before the multicast service for that stream is started. The minimum is 1 and the maximum is 1,000,000.
- **Multicasting Stop Threshold (#viewers):** For a channel that is configured with a Multicast Mode of dynamic, after the multicast service for a stream is running, the multicast service for that stream will continue to run until the number of viewers for that stream drops to the number entered in this field. The minimum is 1 and the maximum is 7200.

  The following is an example of the Multicast Controller Advanced settings:



Step 2 Edit the following fields to configure the Multicast Sender settings of the broadcasting group:

- **Enable Multicast FEC:** Check this check box to enable this feature. When this feature is enabled, FEC data is included in the multicast stream, which allows missing packets to be recovered from a given FEC block using the parity packets instead of having to retransmit the original source data. If this feature is disabled (the check box is not checked), the MC-Receivers will have to perform unicast retransmission to recover lost packets. Enabling FEC may increase bandwidth usage.
- **Multicast FEC Block Size (kB):** The block size, in kB, to use for FEC computation on all NORM streams. The multicast FEC block size and the multicasting FEC repair count determine how much parity information is sent. For example, if the FEC block size is 64 kB and the multicasting FEC repair count

is 8, then for every 64 packets of content sent, 8 packets of repair information are sent. The minimum is 8 kB and the maximum is 255 kB. The default value is 64 kB.

Note The following restriction must be satisfied: Multicast FEC Block Size + Multicasting FEC Repair Count <= 255.

- **Multicasting FEC Repair Count (#):** The repair count to use for FEC computation on all NORM streams. The multicast FEC block size and the multicasting FEC repair count determine how much parity information is sent. For example, if the FEC block size is 64 kB and the multicasting FEC repair count is 8, then for every 64 packets of content sent, 8 packets of repair information are sent. The default block size is 64 kB. The minimum is 1 and the maximum is 255. The default is 8.

  Note The following restriction must be satisfied: Multicast FEC Block Size + Multicasting FEC Repair Count <= 255.

- **Multicast DSCP:** The DSCP byte to use on NORM traffic for all the streams. The minimum value is 0 and the maximum value is 63.
- **Multicast Rate Multiplier:** The multiplier factor by which to increase the multicast rate for each stream. This can be a decimal number in the range from 1 to 10, inclusive. The default is 1.2.

  The following is an example of the Multicast Sender settings:

Step 3 Edit the following fields to configure the Embedded Multicast Client (MC-Receiver) settings of the broadcasting group:

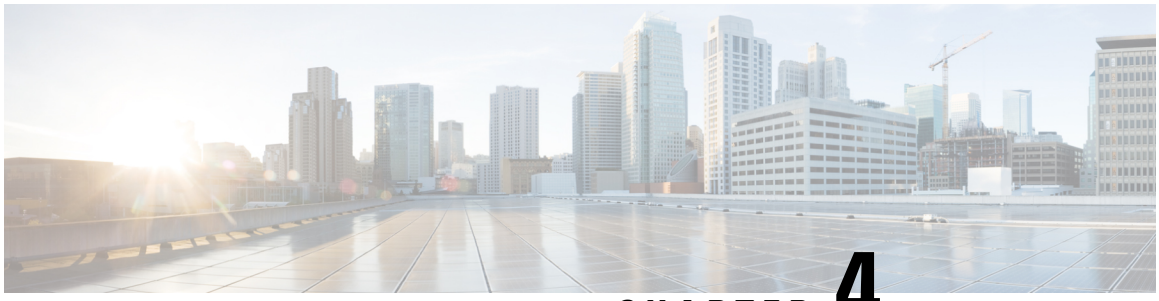
- **Multicast Start Delay (sec):** The number of seconds the MC-Receiver waits after the first segment is delivered on a given stream before joining the multicast stream. The minimum is 0 and the maximum is 600. The default is 30.
- **Multicast Stop Delay (sec):** The number of seconds the MC-Receiver should wait between the last GET for a segment on the stream and when it leaves the multicast stream. The minimum is 30 and the maximum is 864,000 (10 days). The default is 30.
- **Stream Status Interval (sec):** The number of seconds the MC-Receiver waits between sending StreamStatus messages to the Multicast Controller. A value of 0 or -1 indicates that the MC-Receiver must not send time-based StreamStatus messages. The minimum is -1 and the maximum is 900. The default is 300 (5 minutes).
- **Manifest Segment Drops (#segments):** The number of segments the MC-Receiver should drop from the manifest if it supports manifest manipulation. The minimum is 0 and the maximum is 100. The default is 2.
- **Stream Status Active Threshold (sec):** The number of seconds since the most recent GET request for a Multicast-Ready Stream segment before the MC-Receiver considers the stream inactive in its StreamStatus reporting. The minimum is 4 and the maximum is 864,000 (10 days). The default is 30.
- **Disable Proxy Transparency:** Check this check box to have the MC-Receiver disable proxy transparency. If the media player has not been manipulated to request segments directly from the MC-Receiver, do not check this check box to disable proxy transparency. If the media player has been manipulated to request

segments directly from the MC-Receiver, check this check box to disable proxy transparency proxy in the MC-Receiver because it is not needed. Proxy transparency is enabled by default.

- **Stream Status Event Delay (sec):** The number of seconds to wait after a channel change to a multicast-ready stream before sending a StreamStatus message. A value of -1 indicates that the MC-Receiver must not send event-based StreamStatus messages. The minimum is -1 and the maximum is 3600. The default is -1.
- **Refresh Interval (sec):** The number of seconds the MC-Receiver waits between configuration refreshes. The minimum is 10 and the maximum is 241,9200 (4 weeks). The default is 86,400 (1 day).

  The following is an example of the Embedded Multicast Client settings:

Step 4 When you are finished configuring the advanced settings of the broadcasting group, if you are finished configuring the broadcasting group, click **Save**. If you need to make any changes before saving, click **Previous** to go back and edit the channel lineup or the filtering rules.



CHAPTER 4

Managing Broadcasting Groups

After you have added the broadcasting groups to OMD Director and configured them, you may need to add or remove channels to the channel lineup, or you may need to modify the filtering rules or advances settings. This chapter describes how to perform these configuration tasks.

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this chapter, make sure you are logging into the Primary OMD Director instance. If you are logged into the Backup OMD Director instance, you will see "This OMD Director is currently running in backup mode" in the header. If you are logged into a an OMD Director running in Detached mode because of an HA failure, you will see "This OMD Director is currently running in detached mode".

This chapter includes the following sections:

- Managing Broadcasting Groups Overview, on page 33
- View Existing Broadcasting Groups, on page 34
- Add a Broadcasting Group, on page 36
- Edit a Broadcasting Group, on page 36
- Export the Channel Lineup, on page 45
- Delete a Broadcasting Group, on page 46

Managing Broadcasting Groups Overview

From the Media Broadcaster > Broadcasting Groups window you can perform the following management tasks for the broadcasting group:

- View the existing broadcasting groups, including:
  - Members of a group
  - Channel lineup of a group
  - Filtering rules of a group
  - Advanced settings of a group
- Add a broadcasting group

- Edit the broadcasting group settings:
  - Channel lineup
  - Edit the filtering rules of a group
  - Edit the advanced settings of a group
- Export a channel lineup to a CSV file
- Delete a broadcasting group
- Delete channels from a channel lineup.

View Existing Broadcasting Groups

To see a list of existing broadcasting groups and their members, choose **Media Broadcaster > Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of, including the following information for each group:

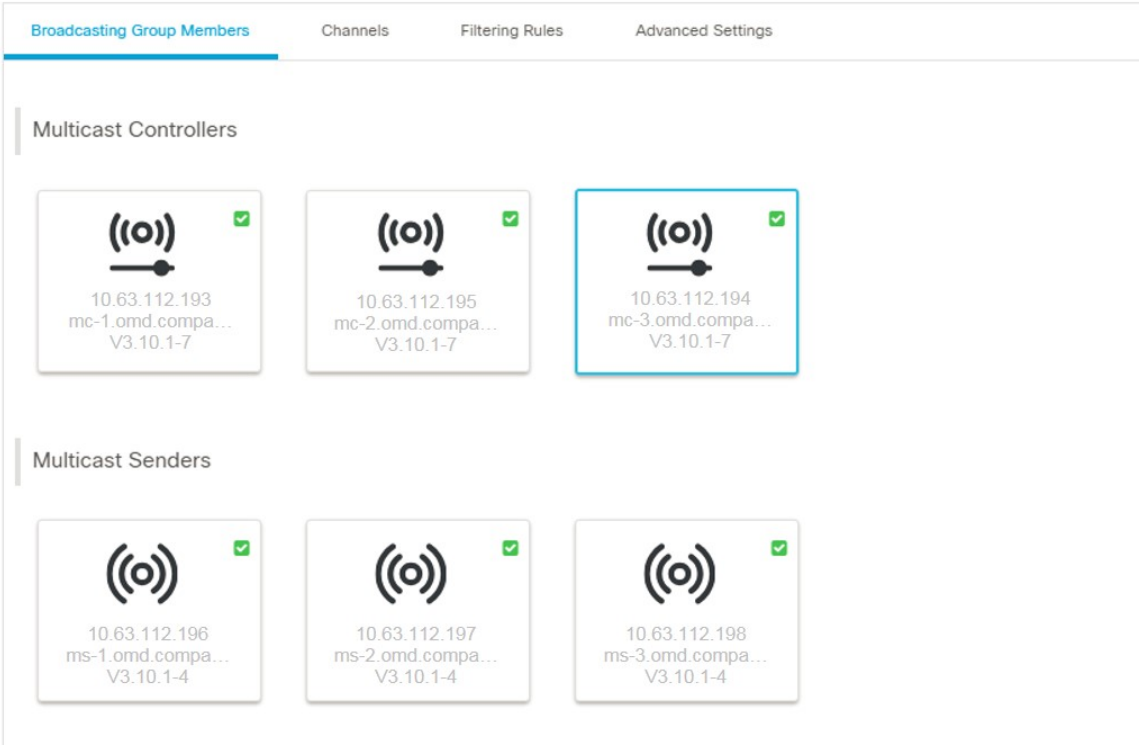
- Name of the group
- Status of the group. A check mark indicates that the broadcasting group is available and a dash indicates that the broadcasting group is unavailable.
- Management address. In an HA configuration, this is the floating IP address of the Broadcaster Configuration Manager (BCM). For a non-HA configuration, this is the IP address of that BCM.
- Number of channels configured for the group.
- Number of Multicast Controllers in the group.
- Number of Multicast Senders in the group.

To see more detailed information about the group, including the channel lineup and the advanced settings, choose a multicasting group from the list. The bottom part of the Broadcasting Groups window shows the following details for the selected multicasting group:

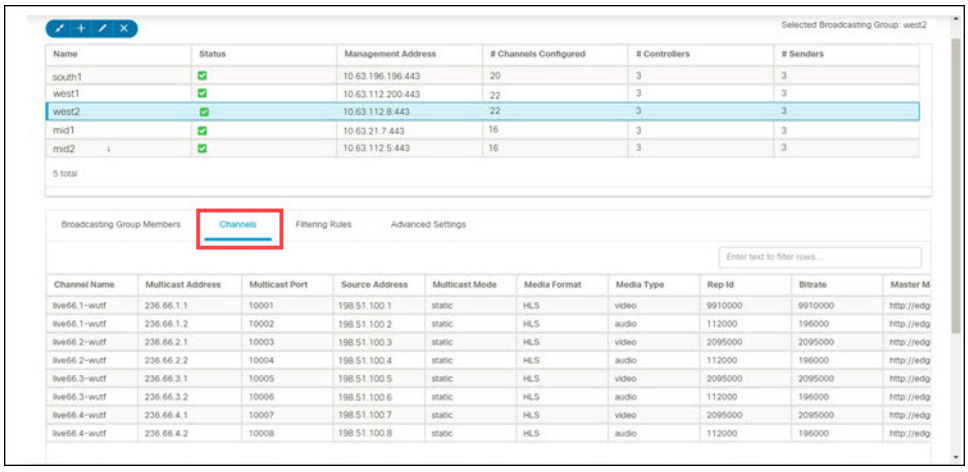
Note From the bottom part of the Broadcasting Groups window you can only view the information for the broadcasting group, you cannot make any changes here. For information on editing the configuration of a broadcasting group, see Edit a Broadcasting Group, on page 36.

- **Broadcasting group members:** This tab shows each Multicast Controller and Multicast Sender that is part of the group. It also displays the following information for each server that is part of the group:
  - IP address
  - Hostname
  - Media Broadcaster software version
  - Status of the server.

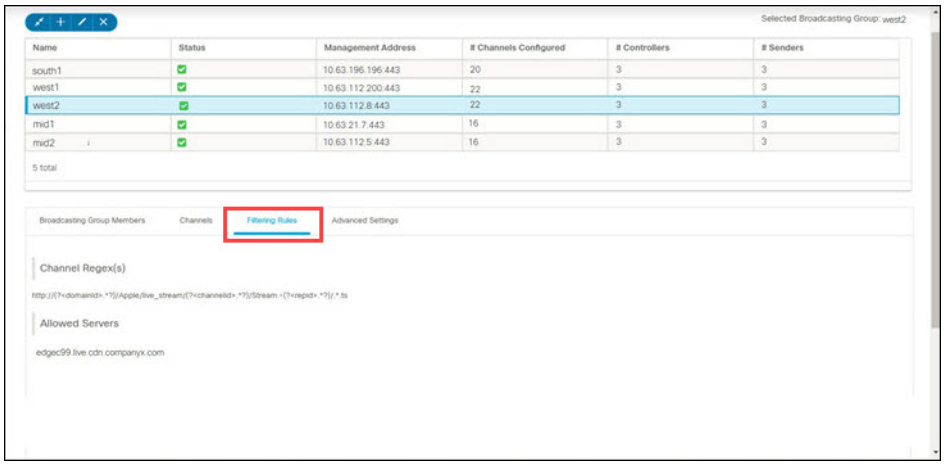
- A check mark in the upper-right hand corner of the server icon means the server is available.
- A dash in the upper-right hand corner of the server icon means the server is unavailable.
    - The Multicast Controller that is highlighted with a blue box is the active Multicast Controller. In the following example, mc-3 is the active Multicast Controller.



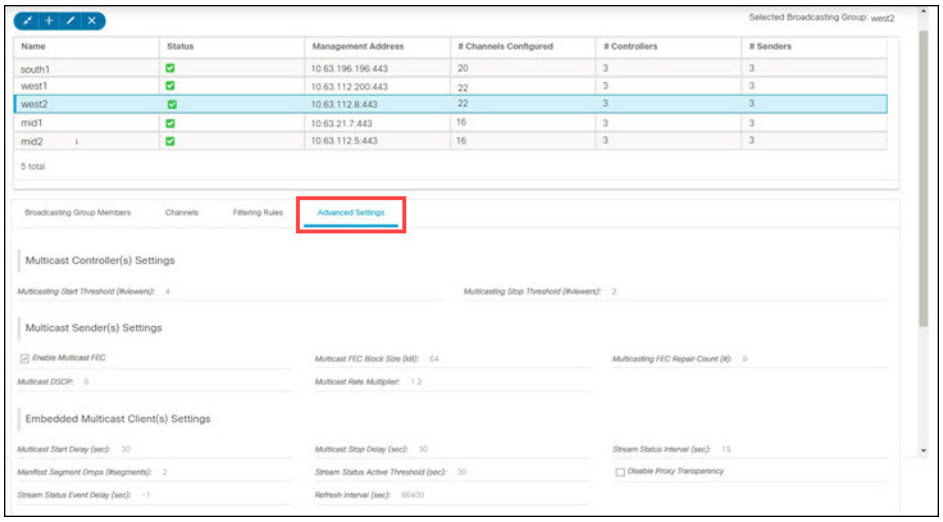
- **Channels:** This tab shows information about the channels that the broadcasting group can multicast.



- **Filtering Rules:** This tab shows the criteria that is used to determine if a URL being requested from a managed HTTP media player is a candidate for multicasting.



- **Advanced Settings:** This tab shows the current settings for the Multicast Controllers, Multicast Senders, and Embedded Multicast Receivers (also referred to as the MC-Receivers) that are part of the broadcasting group. All Multicast Controllers, Multicast Senders, and Embedded Multicast Receivers that are part of the broadcasting group use the same settings.



Add a Broadcasting Group

For information on adding a broadcasting group, see the Configuring Broadcasting Groups chapter.

Edit a Broadcasting Group

From the **Media Broadcaster > Broadcasting Groups** menu you can edit the channel lineup, the filtering rules, and advanced settings of the group.

Note You cannot change the name, broadcasting group address, or broadcasting group port number after a broadcasting group is added.

Note If you are running OMD Director in a HA configuration, you can only make configuration changes from the Primary OMD Director instance. Therefore, to perform the steps in this section, make sure you are logging into the Primary OMD Director instance.

Edit the Channel Lineup

Perform the following steps to edit the channel lineup of the broadcasting group:

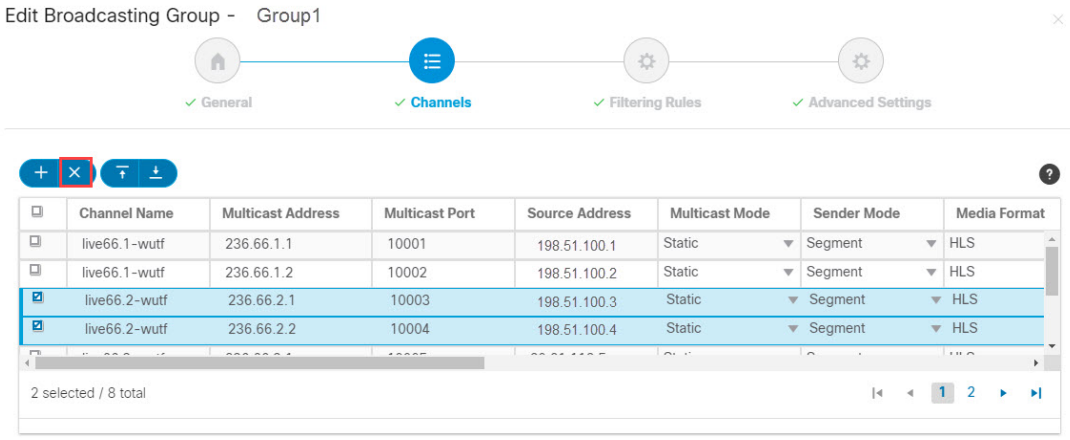
Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group for which you want to edit the channel lineup and click the **Edit** icon.

Step 3 Click the **Channels** icon at the top of the window. From the Channels tab, you can:

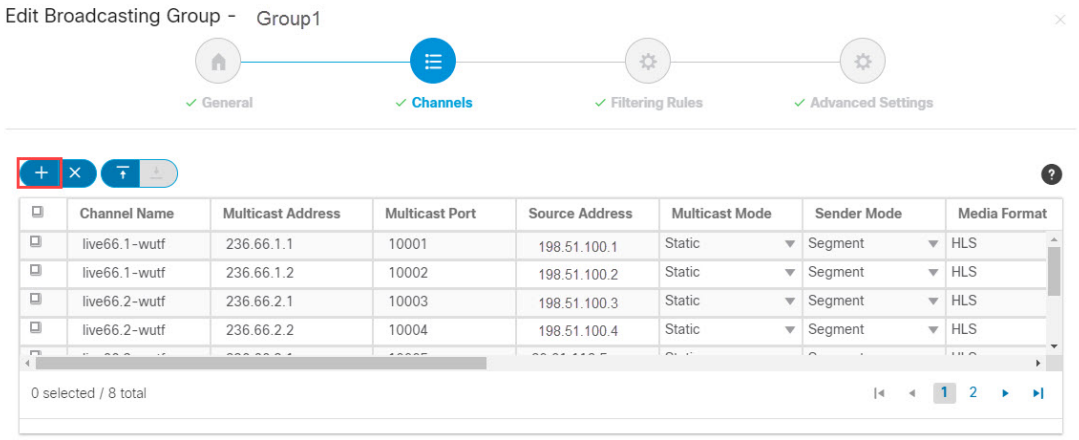
- Edit the settings of any individual channel: In the row of the channel you need to edit, enter the new value for any field you need to change.
- Delete a channel from the list: To delete a channel from the channel list, check the check box for the channels you want to delete and click the **Delete** (x) icon.



- Import channels using a CSV file. For more information on using a CSV file to import a channel lineup, see Define the Channel Lineup, on page 22 in Configuring Broadcasting Groups, on page 19.

Warning If you use a CSV file to import a channel lineup to an already existing configuration, the channel importer will replace all of the existing channels in the list. Before you do an import, you can export all of the exiting channels in the lineup to a CSV file. For more information on exporting the channel lineup, see Export the Channel Lineup, on page 45.

- Add a new channel to the list: To add a single channel to the lineup, click the Add (+) icon. A new row will appear at the bottom of the list.



Enter the following information for the new channel:

- **Channel Name:** Name of the channel. The channel ID is contained in the requested segment URL. This value is used to identify requests from the media player in a managed home that are candidates for multicasting. Each channel ID can have only one audio and one video entry in the channel lineup.
- **Multicast Address:** The multicast address to use when multicasting this linear asset.
- **Multicast Port:** The port number to use when multicasting this linear asset.
- **Source Address:** The IP address the Multicast Sender will use as the source address when multicasting the linear asset.
- **Multicast Mode:** Choose static or dynamic:
  - **static:** The Multicast Controller will tell the Multicast Sender to start multicasting the linear asset at startup.
  - **dynamic:** The Multicast Controller will tell the Multicast Sender to start multicasting the linear asset when the Multicasting Start Threshold has been met. The Multicasting Start Threshold defines how many viewers must be watching a particular stream before the multicast service for that stream is started.

    Note The Multicasting Start Threshold is configured on the **Advanced Settings** tab of the Edit Broadcasting Group wizard.

- **Media Format:** Enter the media format of the channel. This can be HLS, DASH, or HSS.
- **Media Type:** Choose either Audio or Video.
- **Rep Id:** Representation Identifier for this linear asset. The Representation ID is part of the segment URL.
- **Bitrate:** Bitrate of the channel.
- **Master Manifest URL:** The URL of the top level manifest for the linear asset.

Step 4 When you are finished making changes to the channel lineup, click **Save**.

Edit the Filtering Rules

The MC-Receiver uses the information configured on the Filtering Rules tab to identify which requests made by an HTTP media player are relevant to multicasting. The entries in the Allowed Servers field determine on which URLs requested by the media player the MC-Receiver should be further processed using REGEX match.

After the MC-Receiver determines that the URL requested by the media player should be checked for a REGEX match, PERL Compatible Regular Expressions (PCRE) uses the regular expressions configured in the Multicast URL Regex field to determine whether or not the stream being requested by the media player is available via multicast. The domain, content identifier, and bit rate of the URL requested by the media player are compared to the regular expressions configured in the Multicast URL Regex field. If there is a match against one of the configured regular expressions, the content identifier and bit rate portions of the URL are then compared against the same fields in the channel lineup of the broadcasting group. If a match is found, the MC-Receiver will join the multicasting group for that channel.

From the Filtering Rules tab of the Editing Broadcasting Group window, you can:

- Add, edit, and delete the multicast URL Regex entries
- Add, edit, and delete the allowed servers.

Add Multicast URL Regex Entries

Perform the following steps to add a multicast URL Regex entry for the broadcasting group:

Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group for which you want to add a multicast URL Regex entry and click the **Edit** icon.

Step 3 Click the **Filtering Rules** icon at the top of the window.

Step 4 Click the **Add** (+) button next to Multicast ULR Regex. A new blank field appears. In this field, enter a new multicast URL Regex entry. For example:

```
http://(?<domainId>.*?)/Apple-live/stream/(?<channelid>.*?)/Stream.-(?<repid>.*?)/.*.ts
```

Step 5 Click **Save**.

Edit Multicast URL Regex Entries

Perform the following steps to edit a multicast URL Regex entry for the broadcasting group:

Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group for which you want to edit a multicast URL Regex entry and click the **Edit** icon.

Step 3 Click the **Filtering Rules** icon at the top of the window.

Step 4 Make the necessary changes to an existing multicast URL Regex and click **Save**.

Delete Multicast URL Regex Entries

Perform the following steps to delete a multicast URL Regex entry for the broadcasting group:

Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group for which you want to delete a multicast URL Regex entry and click the **Edit** icon.

Step 3 Click the **Filtering Rules** icon at the top of the window.

Step 4 Click the **Delete** (X) button at then end of the row for the Multicast ULR Regex you want to delete.

Step 5 Click **Save**.

Add an Allowed Server

The entries in the Allowed Servers field determine on which URLs requested by the media player the MC-Receiver should be further processed using REGEX match. Perform the following steps to add an allowed server for the broadcasting group:

Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group for which you want to add an allowed server and click the **Edit** icon.

Step 3 Click the **Filtering Rules** icon at the top of the window.

Step 4 Click the **Add** (+) button next to Allowed Servers. A new blank field appears. In this field, enter a the IP address of the new server to match against.

Step 5 Click **Save**.

Edit an Allowed Server

Perform the following steps to edit an allowed server for the broadcasting group:

Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group for which you want to edit an allowed server and click the **Edit** icon.

Step 3 Click the **Filtering Rules** icon at the top of the window.

Step 4 Make the necessary changes to an existing allowed server and click **Save**.

Delete an Allowed Server

Perform the following steps to delete an allowed server for the broadcasting group:

Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group for which you want to delete an allowed server and click the **Edit** icon.

Step 3 Click the **Filtering Rules** icon at the top of the window.

Step 4 Click the **Delete** (X) button at then end of the row for the allowed server you want to delete.

Step 5 Click **Save**.

Edit the Advanced Settings

The advanced settings of the broadcasting group contain settings that control the functionality of the Multicast Controllers, Multicast Senders, and Embedded Multicast Clients of the broadcasting group. Perform the following steps to edit these settings:

Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group for which you want to edit the advanced settings and click the **Edit** icon.

Step 3 Click the **Advanced Settings** icon at the top of the window. Use the following table to make any necessary changes to the settings.

Table 2: Broadcasting Group Advanced Settings

Component	Setting	Description
Multicast Controller	Multicasting Start Threshold (#viewers)	For a channel that is configured with a Multicast Mode of dynamic, enter the minimum number of viewers that must be watching that stream before the multicast service for that stream is started. The minimum is 1 and the maximum is 1,000,000.
Multicast Controller	Multicasting Stop Threshold (#viewers)	For a channel that is configured with a Multicast Mode of dynamic, after the multicast service for a stream is running, the multicast service for that stream will continue to run until the number of viewers for that stream drops to the number entered in this field. The minimum is 1 and the maximum is 7200.
Multicast Sender	Enable Multicast FEC	Check this check box to enable this feature. When this feature is enabled, FEC data is included in the multicast stream, which allows missing packets to be recovered from a given FEC block using the parity packets instead of having to retransmit the original source data. If this feature is disabled (the check box is not checked), the MC-Receivers will have to perform unicast retransmission to recover lost packets. Enabling FEC may increase bandwidth usage.

Component	Setting	Description
Multicast Sender	Multicast FEC Block Size (kB)	The block size, in kB, to use for FEC computation on all NORM streams. The multicast FEC block size and the multicasting FEC repair count determine how much parity information is sent. For example, if the FEC block size is 64 kB and the multicasting FEC repair count is 8, then for every 64 packets of content sent, 8 packets of repair information are sent. The minimum is 8 kB and the maximum is 255 kB. The default value is 64 kB. **Note** The following restriction must be satisfied: Multicast FEC Block Size + Multicasting FEC Repair Count <= 255.
Multicast Sender	Multicasting FEC Repair Count (#)	The repair count to use for FEC computation on all NORM streams. The multicast FEC block size and the multicasting FEC repair count determine how much parity information is sent. For example, if the FEC block size is 64 kB and the multicasting FEC repair count is 8, then for every 64 packets of content sent, 8 packets of repair information are sent. The default block size is 64 kB. The minimum is 1 and the maximum is 255. The default is 8. **Note** The following restriction must be satisfied: Multicast FEC Block Size + Multicasting FEC Repair Count <= 255.
Multicast Sender	Multicast DSCP	The DSCP byte to use on NORM traffic for all the streams. The minimum value is 0 and the maximum value is 63.

Component	Setting	Description
Multicast Sender	Multicast Rate Multiplier	The multiplier factor by which to increase the multicast rate for each stream. This can be a decimal number in the range from 1 to 10, inclusive. The default is 1.2.
Embedded Multicast Client	Multicast Start Delay (sec)	The number of seconds the MC-Receiver waits after the first segment is delivered on a given stream before joining the multicast stream. The minimum is 0 and the maximum is 600. The default is 30.
Embedded Multicast Client	Multicast Stop Delay (sec)	The number of seconds the MC-Receiver should wait between the last GET for a segment on the stream and when it leaves the multicast stream. The minimum is 30 and the maximum is 864,000 (10 days). The default is 30.
Embedded Multicast Client	Stream Status Interval (sec)	The number of seconds the MC-Receiver waits between sending StreamStatus messages to the Multicast Controller. A value of 0 or -1 indicates that the MC-Receiver must not send time-based StreamStatus messages. The minimum is -1 and the maximum is 900. The default is 300 (5 minutes.)
Embedded Multicast Client	Manifest Segment Drops (#segments)	The number of segments the MC-Receiver should drop from the manifest if it supports manifest manipulation. The minimum is 0 and the maximum is 100.
Embedded Multicast Client	Stream Status Active Threshold (sec)	The number of seconds since the most recent GET request for a Multicast-Ready Stream segment before the MC-Receiver considers the stream inactive in its StreamStatus reporting. The minimum is 4 and the maximum is 864,000 (10 days). The default is 30.

Component	Setting	Description
Embedded Multicast Client	Disable Proxy Transparency	Check this check box to have the MC-Receiver disable proxy transparency. If the media player has not been manipulated to request segments directly from the MC-Receiver, do not check this check box to disable proxy transparency. If the media player has been manipulated to request segments directly from the MC-Receiver, check this check box to disable proxy transparency proxy in the MC-Receiver because it is not needed. Proxy transparency is enabled by default.
Embedded Multicast Client	Stream Status Event Delay (sec)	The number of seconds to wait after a channel change to a multicast-ready stream before sending a StreamStatus message. A value of -1 indicates that the MC-Receiver must not send event-based StreamStatus messages. The minimum is -1 and the maximum is 3600. The default is -1.
Embedded Multicast Client	Refresh Interval (sec)	The number of seconds the MC-Receiver waits between configuration refreshes. The minimum is 10 and the maximum is 604,800 (1 week). The default is 86,400 (1 day).

Step 4 When you are finished making changed, click **Save**.

Export the Channel Lineup

If you use a CSV file to import a channel lineup to an already existing configuration, the channel importer will replace all of the existing channels in the channel lineup for that broadcasting group. If you need to import a group of channels to an already existing channel lineup, you can first export the existing channel lineup and use that CSV file to add additional channels to. When you are done adding the additional channels, you can then use that CSV file to import all of the channels.

Also, if you have manually added channels to the channel lineup, you may want to export the channel lineup to a CSV file so you have a backup copy of all of the channels in a CSV file.

Perform the following steps to export an existing channel lineup of a broadcasting group:

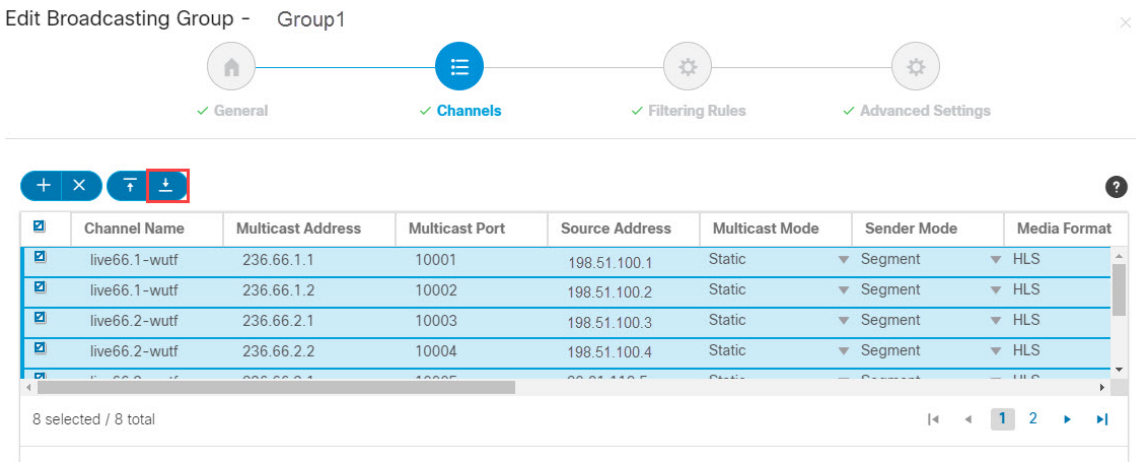
Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From the list of broadcasting groups, choose the broadcasting group for which you want to export the channel lineup and click the **Edit** icon.

Step 3 Click the **Channels** icon at the top of the window.

Step 4 From the list of channels, check the check box for the channels you want to export. To select all channels, click the check box in the column header. Click the **Export Channels** icon.



Step 5 In the window that appears, browse for a location to save the file, enter a name for the file, and click **Save**.

Delete a Broadcasting Group

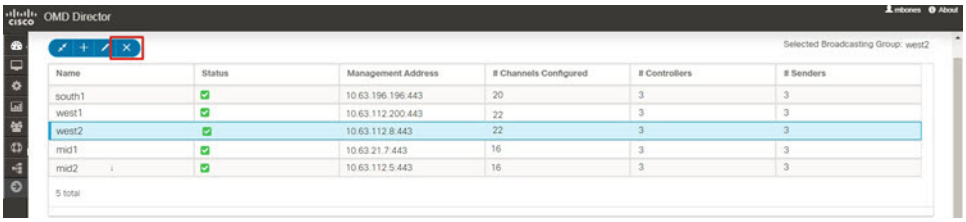
Perform the following steps to delete a broadcasting group.

Note Deleting a broadcasting group from OMD Director only removes the references to that group from OMD Director. The actual Multicast Controllers, Multicast Senders, and Multicast Receivers still exist and are still configured.

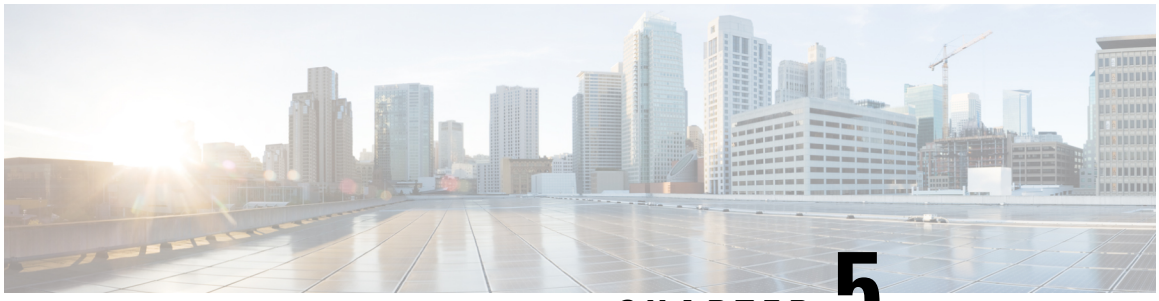
Procedure

Step 1 Choose **Media Broadcaster** > **Broadcasting Groups**. The window that appears has a table that displays the broadcasting groups that OMD Director is aware of.

Step 2 From this list of broadcasting groups, choose the broadcasting group that you want to delete and click the **Delete** icon.



Step 3 In the Delete Broadcasting Group dialog box, click **Confirm** to delete the group.



CHAPTER 5

Media Broadcaster Monitoring

OMD Director enables you to see a server-based view of system-level statistics for a specific Media Broadcaster Multicast Controller or Multicast Sender. This chapter looks at the different information that you can view from the Monitor menu in OMD Director for Media Broadcaster.

Note There is additional information that can be viewed from the Monitor menu for the servers in a Media Streamer deployment. This guide only covers information for Media Broadcaster. For more information on the data available from the Monitor menu for a Media Streamer deployment, please see the *Cisco Media Streamer User Guide*.

This chapter includes the following sections:

- Server Metrics, on page 49
- Alarms, on page 53
- Mute Alarms, on page 62

Server Metrics

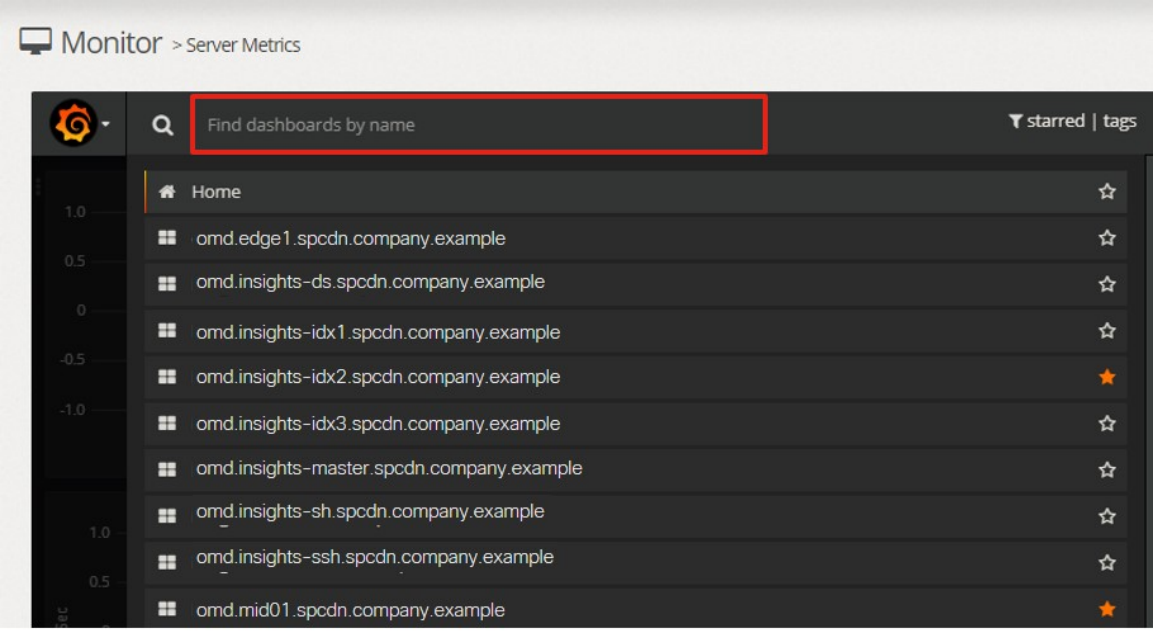
Server metrics enables you to see a server-based view of system-level statistics for a specific Media Broadcaster server. To see these metrics, choose **Monitor** > **Server Metrics**. At that point, OMD Manager will open a pane that retrieves the server metrics from OMD Monitor.

Note The first time that you choose **Monitor > Server Metrics**, you will be prompted to log in to Grafana. Grafana is an open source graphical interface used for visualizing time series data through dashboards, rich graphing and alerting, and is the user interface for OMD Monitor. The default username and password will depend on the installation. For more information, please refer to the *Cisco Media Streamer and Cisco Media Broadcaster Installation and Upgrade Guide*. This login is only required once per browser. After your initial login to Grafana, you can save your username and password in the browser, which eliminates the need to authenticate every time you wish to view the Server Metrics page.

The Home Dashboard that appears shows you any server dashboards that you have marked as favorite (starred) and any recently viewed server dashboards.

To see the system-level statistics for a specific server in the OMD environment, do one of the following:

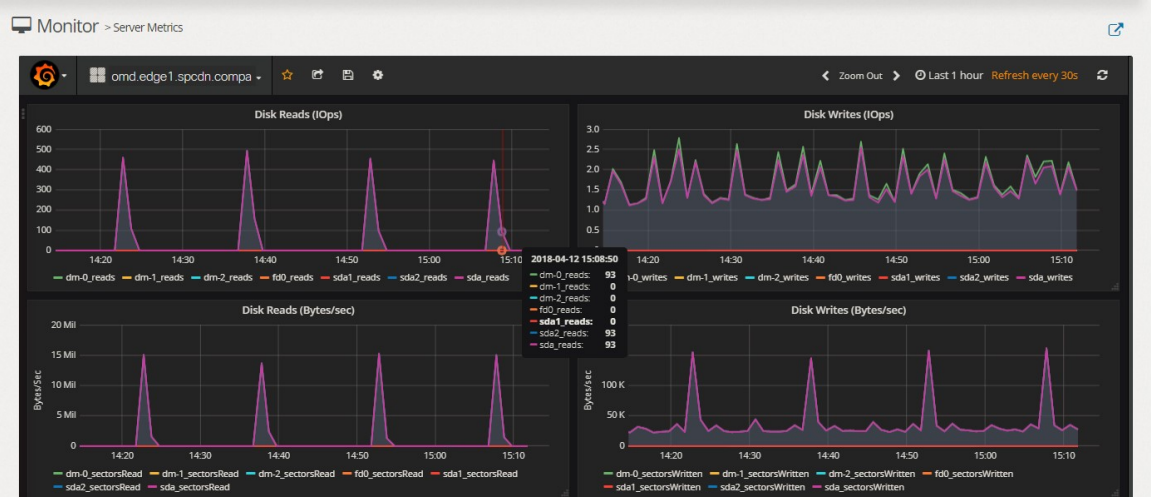
- Click the link for the server dashboard under Starred Dashboards if it exists.
- Click the link for the server dashboard under Recently Viewed Dashboards if it exists.
- At the top of the Home dashboard, choose the server from the Home drop-down list. You can filter the list of servers by entering part of the server name in the Find Dashboard by Name text box at the top of the Home drop-down list, as seen below.



From the server dashboard you can see the following information about that server:

- Disk reads based on IO per second and bytes per second
- Disk writes based on IO per second and bytes per second
- Ingress and egress bandwidth
- CPU usage and CPU load average
- Memory usage
- Disk usage

The following is an example of the server dashboard:

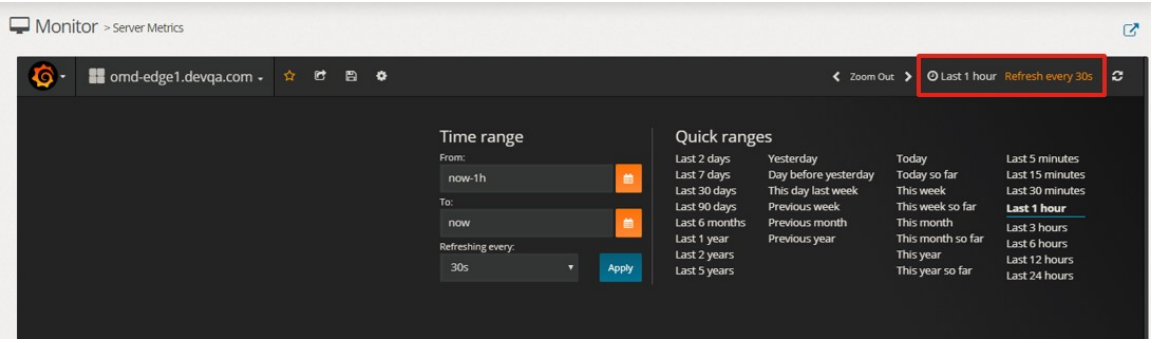


Change Time Range and Interval

By default, the last hour of statistics is displayed and are refreshed every five minutes. To see the statistics for a different time frame and optionally change the refresh rate, perform the following steps:

Procedure

Step 1 Click the time frame icon in the tool bar. This will show the Time Range section of the dashboard at the top of the dashboard.



Step 2 From the Time Range panel you can choose a preconfigured time range from the **Quick ranges** area or you can create a custom time range in the **Time range** area. To configure a custom time range, perform the following steps:

a) Use the calendar icon to choose a From and To date.

Note Optionally you can manually enter a date. If you manually enter a date, it must be in the following format: year-month-date hours:minutes:seconds, where year, month, and date are numbers. The year can be either a 2 digit or 4 digit number and the time argument is optional.

b) Optionally choose a different refresh interval from the Refreshing Every drop-down list. The default is 5 minutes.

c) Click **Apply** to apply the changes and close the Time Range panel.

Step 3 To change the refresh interval of a preconfigured time range, perform the following steps:

a) Click the time frame icon in the tool bar to expand the Time Range panel.

b) From the Time Range panel, click the preconfigured time range in the **Quick ranges** area that you want to change. This will change the time range and close the Time Range panel.

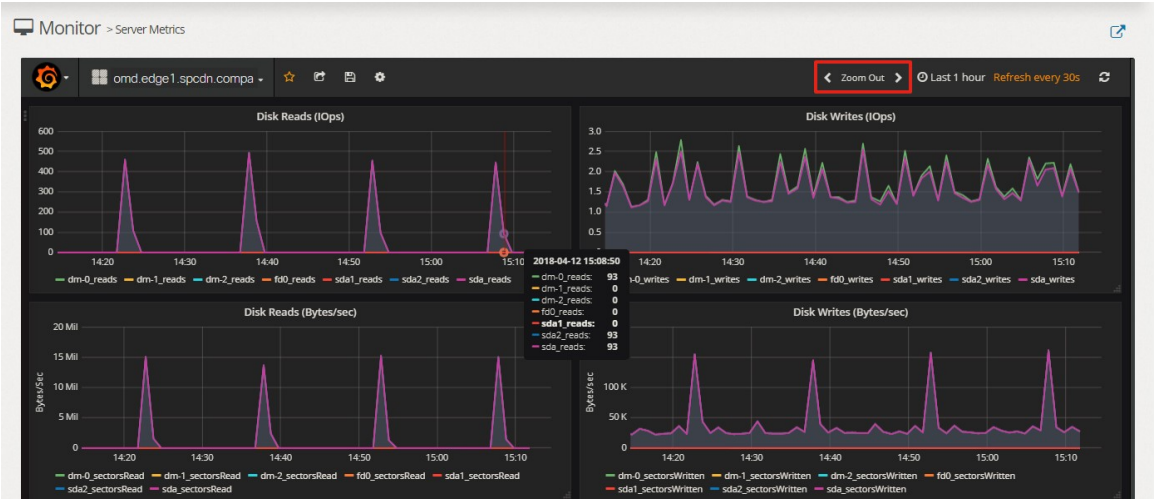
c) Click the time frame icon in the tool bar again to expand the Time Range panel again.

d) From the **Refreshing Every** drop-down list choose a new refresh interval and click **Apply**.

Note The new time range and refresh interval are reset to the defaults as soon as you move to a different dashboard.

Shift Time and Zoom Time

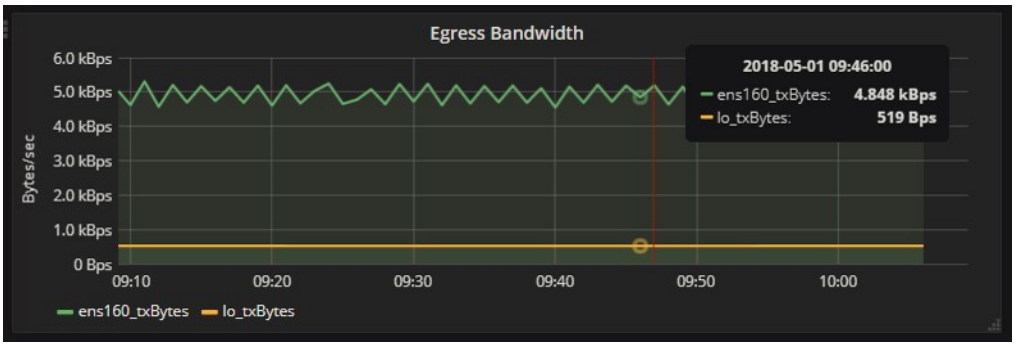
You can use the shift time (left and right arrows) and Zoom Out icons at the top of the toolbar to change the time range represented in the graphs without going into the Time Range panel.



When you click the Zoom Out icon, the time range that is displayed in the graph will double, based on the current time range that is selected. Every time you click the Zoom Out icon, it doubles the time range. For example, if the time range is set to the last 15 minutes, the first time you click the Zoom Out icon, the time range will increase to the last 30 minutes. The second time that you click the Zoom Out icon it will increase to 60 minutes.

Mouse Over

If you hover the mouse over the graph at a specific point, it will show you the value represented in the graph for that specific date and time.



Alarms

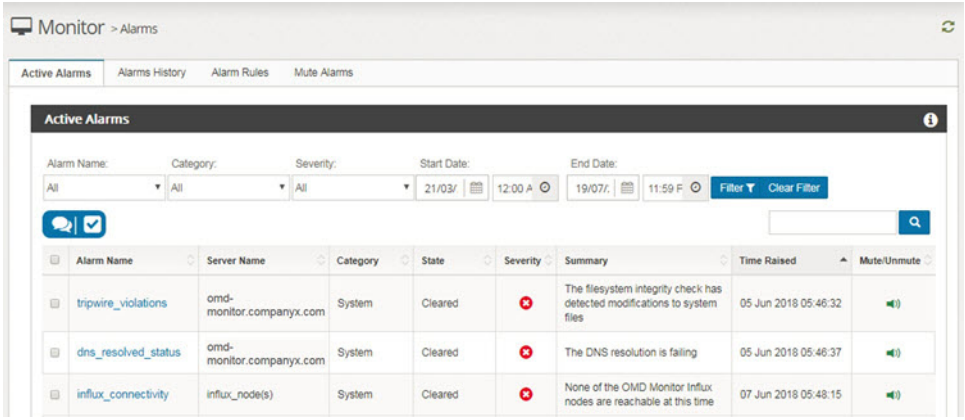
The Alarms page displays the OMD system alarms that have been raised in the OMD environment, based on configured thresholds. From the Alarms pane you can do the following:

- View the active alarms
- View the alarm history
- Configure thresholds for the alarms
- Mute alarms

Note If OMD Director is running in an HA configuration, you can view and filter all of the information available in the Alarms pages from both the Primary and Backup OMD Director instance. However, you cannot acknowledge or clear alarms, configure thresholds for alarms, or mute alarms if you are logged into an OMD Director instance running in Backup mode. If your OMD Director instance is in Detached mode because of a Director instance failure, you can view and filter all of the information available in the Alarms pages and you can also acknowledge, clear, and save alarms.

View Active Alarms

To view the OMD system alarms, choose **Monitor** > **Alarms**. The default tab that is displayed is the **Active Alarms** tab. From this tab you can see the active alarms. The Active Alarms page displays information about unresolved notifications in the OMD system.



Each alarm will have one of the following states:

- **New:** This is an alarm that has not yet been cleared or acknowledged.
- **Cleared:** This is an alarm that has been cleared in the backend but not yet acknowledged by a user in OMD Director.
- **Acknowledged:** This is an alarm that has been acknowledged by a user in OMD Director but has not yet been cleared by the backend.

Note Alarms that are cleared in the backend and have been acknowledged by the user in OMD Director are considered resolved. Resolved alarms do not appear in the Active Alarms tab they appear in the Alarms History Tab.

Each alarm will have one of the following severities:

- **Critical:** This is an alarm that has not yet been cleared or acknowledged.
- **Warning:** This is an alarm that has been cleared in the backend but not yet acknowledged by a user in OMD Director.
- **Acknowledged:** This is an alarm that has been acknowledged by a user in OMD Director but has not yet been cleared by the backend.
- **Resolved:** An alarm is considered resolved when it is cleared in the backend and it is acknowledged by the user in OMD Director. Resolved alarms do not appear in the Active Notifications section they appear in the Alarms History section.

The Notifications column also shows whether the alarm is muted. For details on how to mute or unmute alarms, see Mute Alarms, on page 62.

Acknowledge an Alarm

To resolve a cleared alarm, which will remove it from the Active Alarms tab and save it in the alarms history, you must acknowledge the alarm. Follow these steps to acknowledge an alarm:

Note If you are running OMD Director in an HA configuration, you cannot acknowledge alarms from an OMD Director instance in Backup mode. You can acknowledge an alarm from an OMD Director instance in Primary or Detached mode.

Procedure

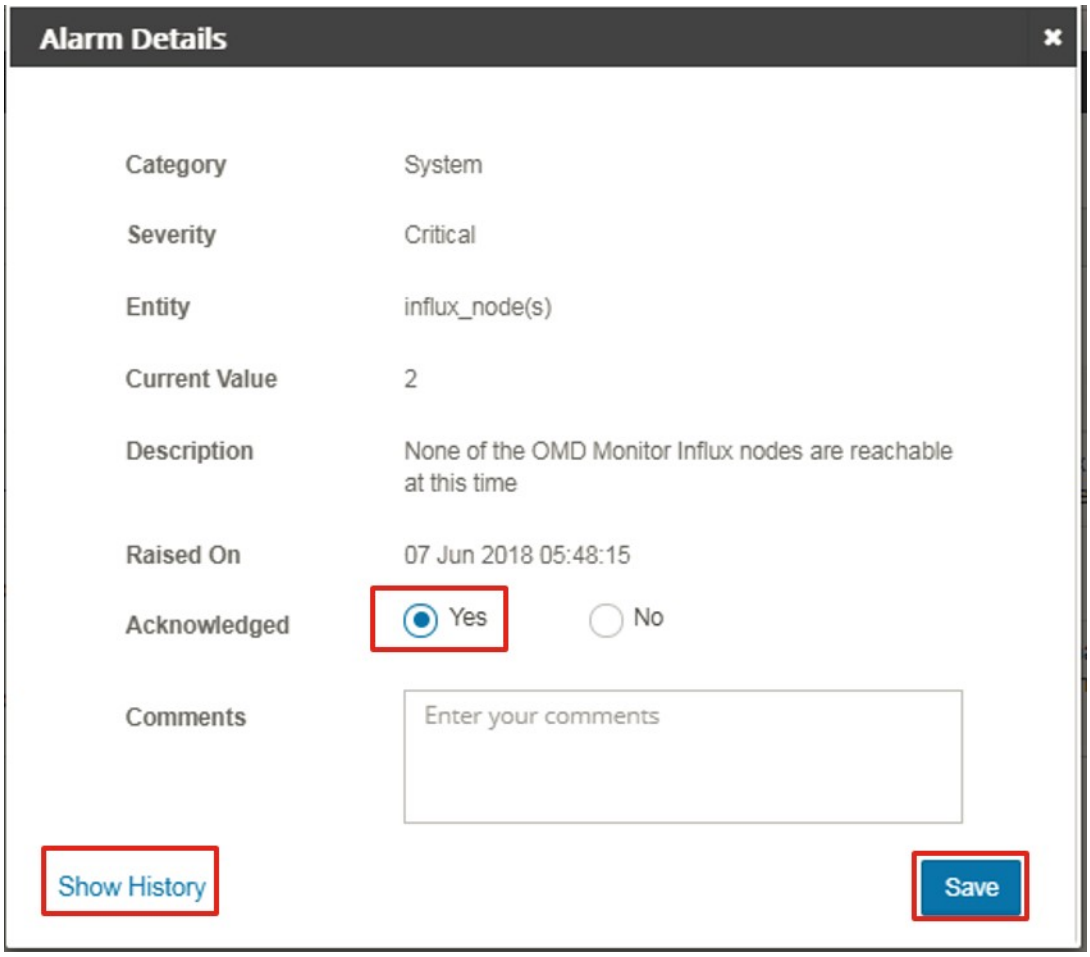
Step 1 Click the link in the Alarm Name column for the alarm that you want to acknowledge. The Alarm Details window appears.

Step 2 In the Alarms Details window to see a history of the Alarm before you acknowledge it, click **Show History**. If the alarm has been cleared by the backend, it will show you the date and time that the alarm was cleared.

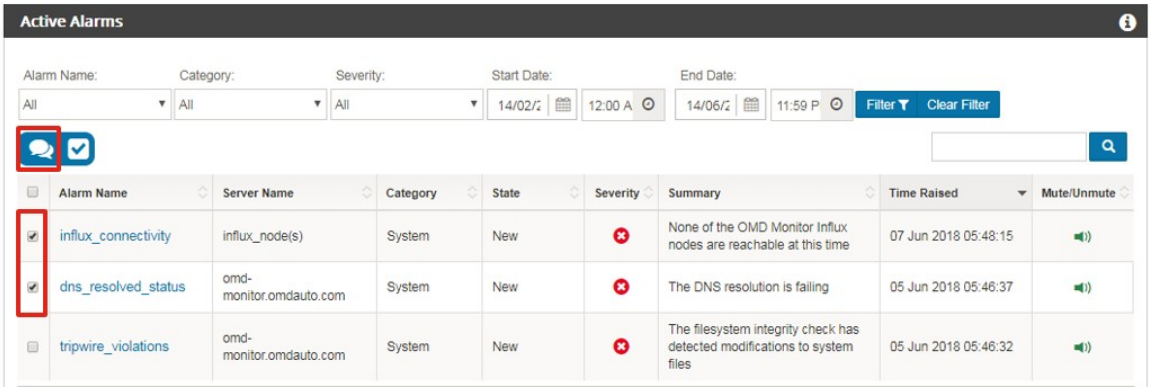
Step 3 Click **Yes** for Acknowledged.

Step 4 Optionally enter a comment in the Comment field.

Step 5 Click **Save**.



Step 6 To acknowledge multiple alarms at the same time, check the check box for each alarm that you want to acknowledge and then click the Acknowledge button. To acknowledge all of the alarms, check the check box in the column header and then click the Acknowledge button.



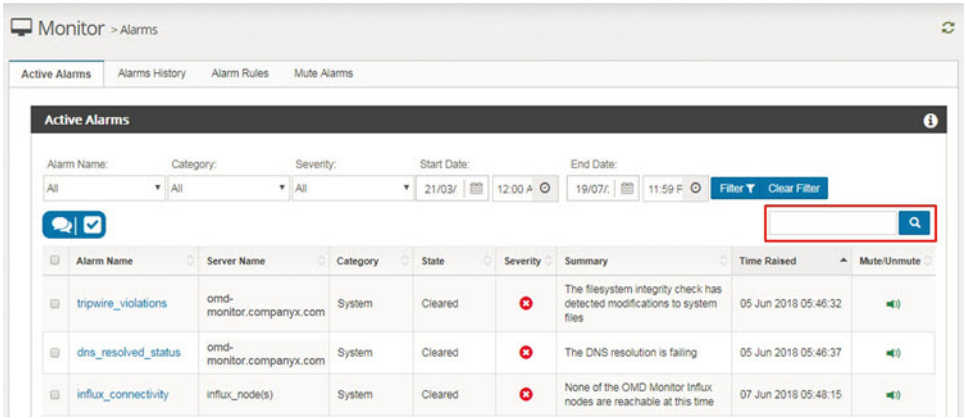
Step 7 In the Alarm Acknowledge Comments window that appears, enter a comment and click **Save**.

Note If you acknowledge an alarm that has not been cleared by the backend, it will remain in the Active Notifications area and will show a state of Acknowledged.

Search for an Alarm

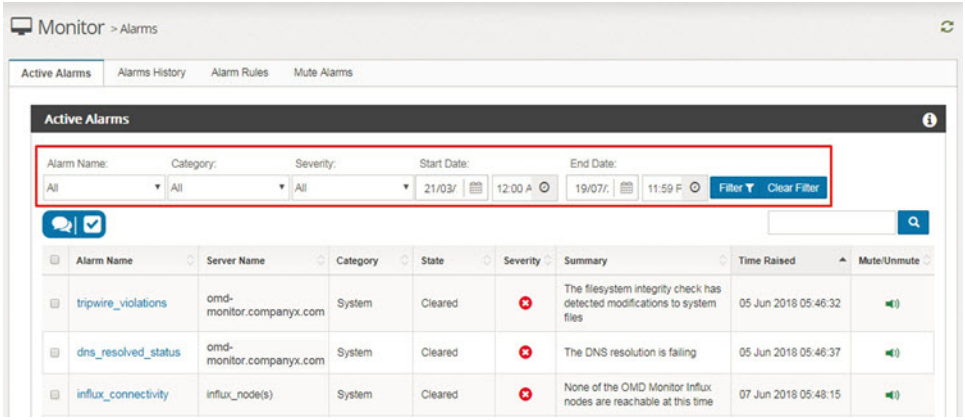
You can also search for alarms by entering text in the search field at the top of the Active Notifications section. The text that you enter is searched for in all of the columns. To search based on the severity of the alarm, enter the severity level you are looking for: critical, warning, informational, or debug.

Note Searches are case-sensitive.



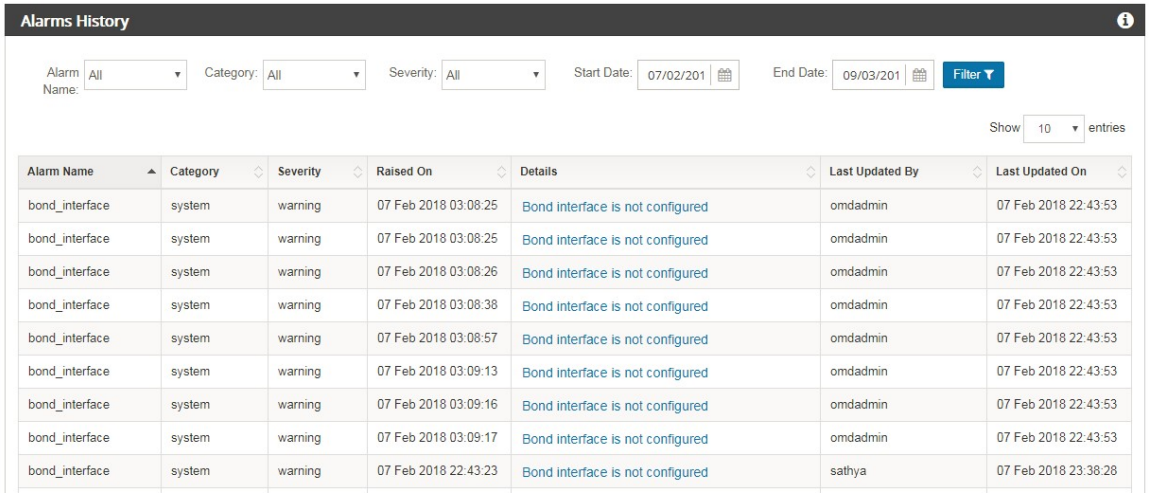
Filter an Alarm

You can also filter the list of alarms by name, category, severity, and date. Enter values in the filter toolbar at the top of the Active Alarms tab and click **Filter**.



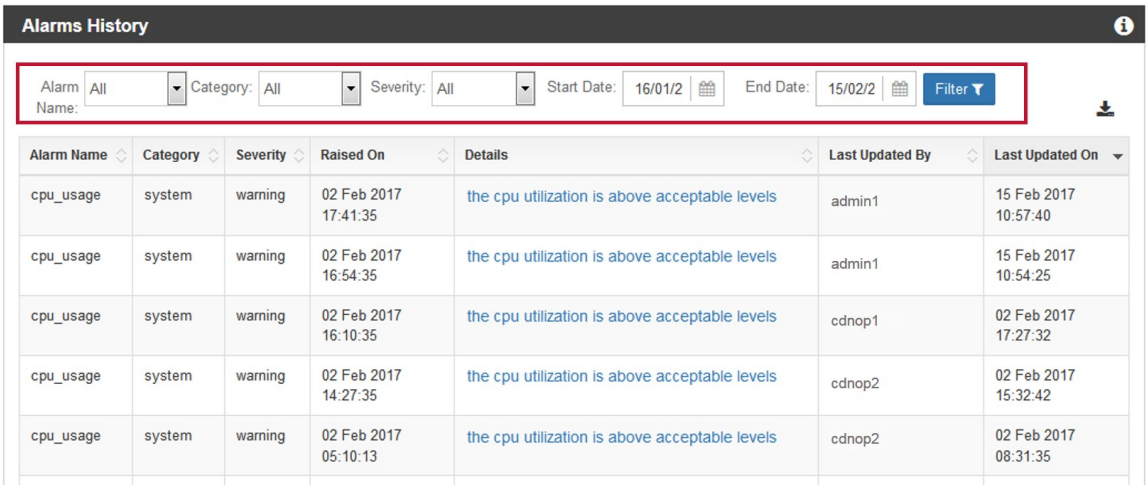
Alarms History

The Alarms History tab from the **Monitor > Alarms** page displays resolved alarms. An alarm is considered resolved when it is cleared by the backend and acknowledged by a user in OMD Director.



Filter Alarms History

By default the Alarms History tab shows the resolved alarms for the past 60 days, but you can change that date range. You can also filter the list of alarms by name, category, and severity. To change the date range that is displayed or to filter based on the alarm name, category, or severity, enter the values in the toolbar at the top of the Alarms History tab and click **Filter**.

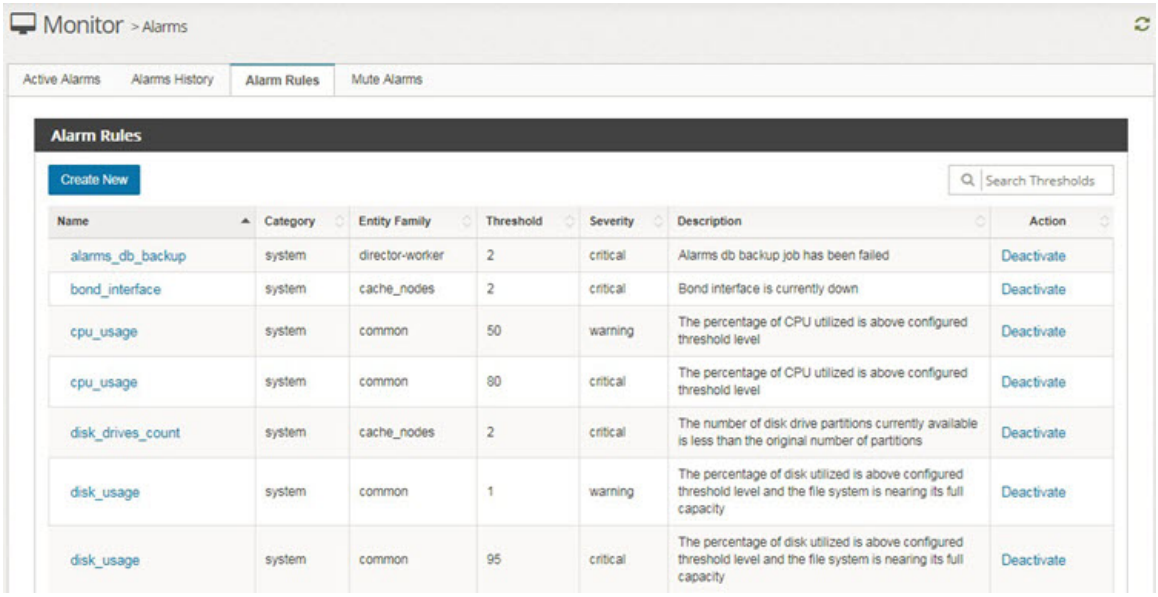


Configure Alarm Rules

All notifications are generated based on the rules that are configured for the alarms. These rules are configured by editing or creating a new alarm rule. An alarm can have multiple rules configured for it to send notifications about different severity levels. To view the existing alarm rules and to create new alarm rules, from the **Monitor > Alarms** page, click the **Alarm Rules** tab.

Note The Appendix: OMD Director Alarms and Remediation, on page 95 describes the default checks and thresholds that are run by the monitor-client service on the OMD Monitor clients that you can view and deactivate in OMD Director from the **Alarms Rules** tab.

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this chapter, make sure you are logging into the Primary OMD Director instance.

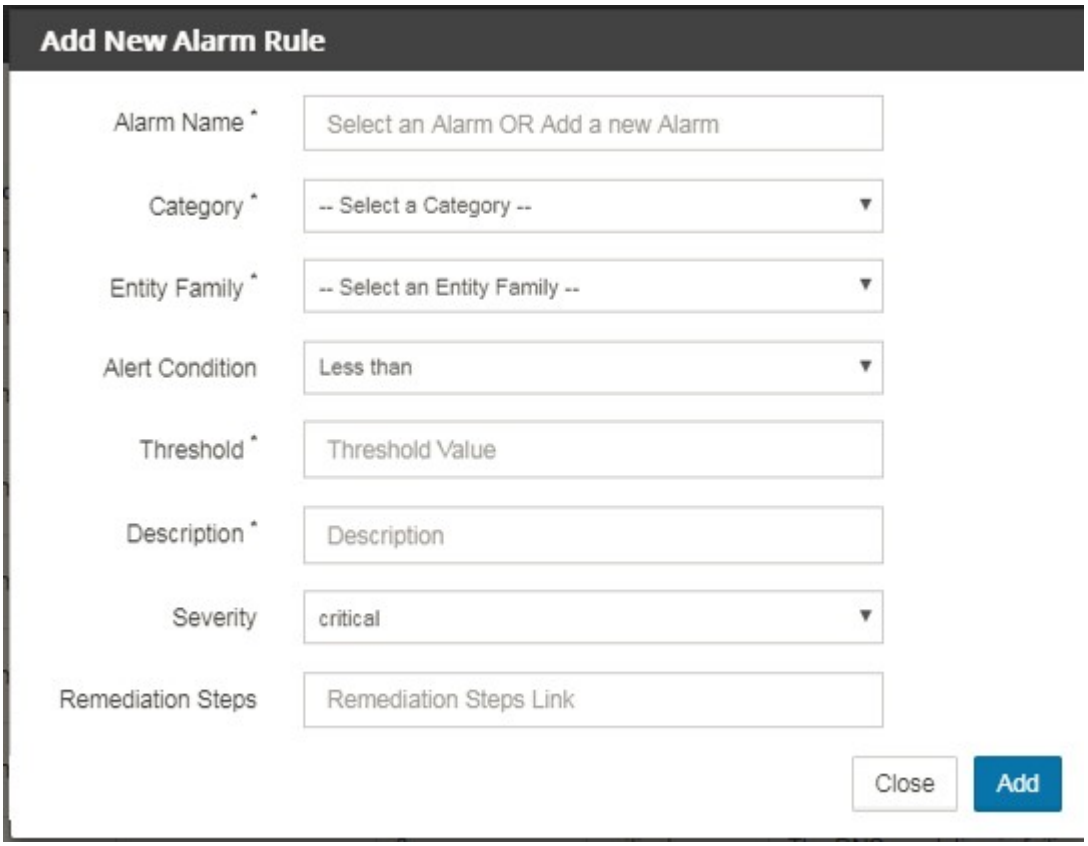


Create New Alarm Rule

Follow these steps to create a new alarm rule for an alarm:

Procedure

Step 1 Click the **Create New** button. The Add New Alarm Rule window appears.



Step 2 In the Add New Alarm Rule window, configure the following fields:

- **Alarm Name:** Choose an alarm from the auto-populated alarms list for which you want to create the rule.
- **Category:** Choose the category. Currently the only category available is System.
- **Entity Family:** Choose the entity family to which this rule will apply. This determines to which CDN elements this rule will apply.
- **Alert Condition:** Choose the Alert Condition from the following:
  - Less than
  - Greater than
  - Equal to
  - Less than or Equal to
  - Greater than or Equal to
- **Threshold:** Enter the value that should trigger the notification based on the Alert Condition.
- **Description:** Enter a description for the rule. It is helpful if the description includes information about the threshold value that needs to be reached to trigger the notification.
- **Severity:** Choose the severity level to assign to this rule. The severity levels are:

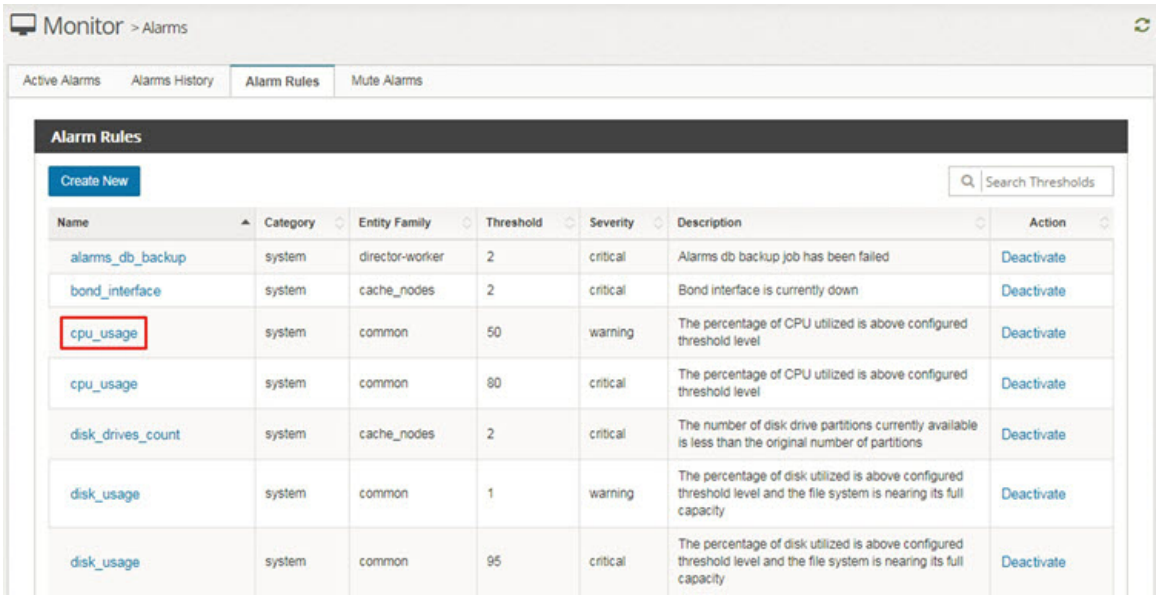
- Critical
- Warning
- Informational
- Debug

- **Remediation Steps:** Optionally enter a URL in this field that points to instructions for the remediation of the alarm. This URL will be included in any email notification that is triggered by this rule. For more information on how to configure which alarms you would like to receive notifications for and how to receive them, see Notification Settings, on page 86.

Step 3 Click **Add** to save the new alarm rule.

Edit an Alarm Rule

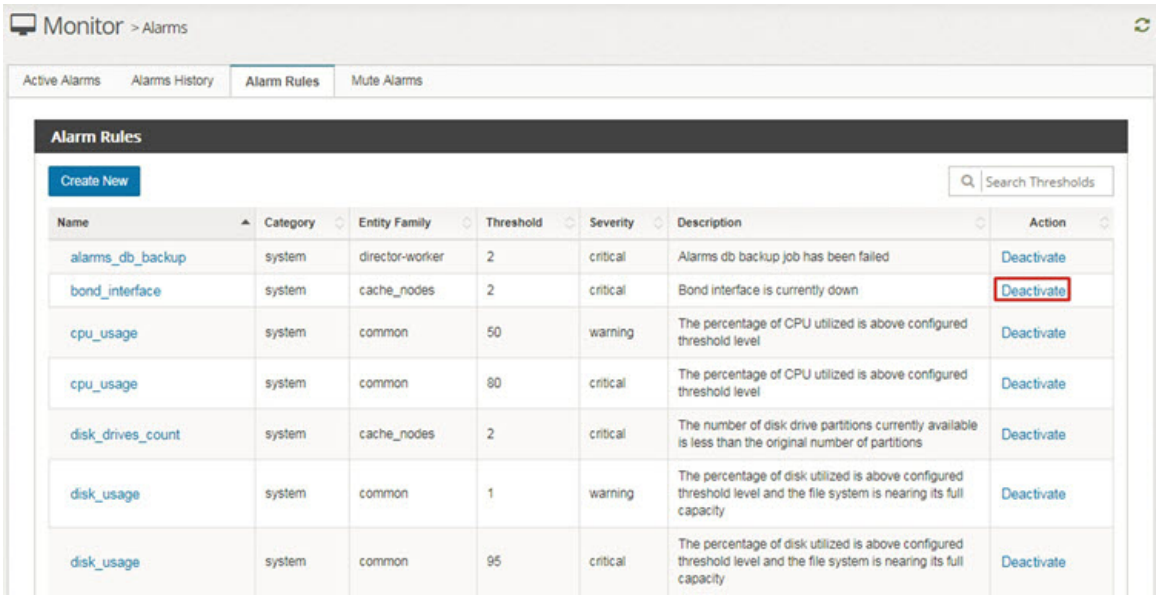
To edit an existing alarm rule, click the name of the alarm rule you want to edit.



The edit panel for the rule expands. From this window you can edit the description, alert condition and threshold value, severity, and link for remediation steps. When you are done making changes, click the **check mark** icon. To cancel the changes, click the **x** icon.

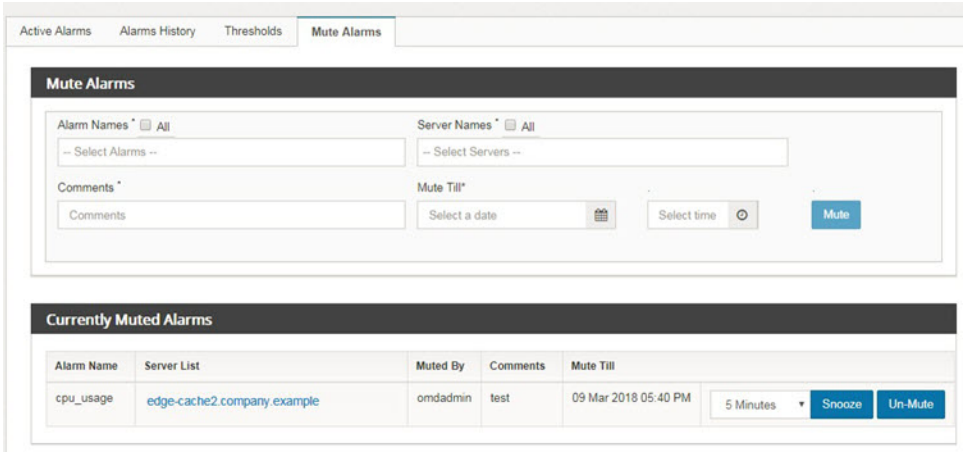
Deactivate an Alarm Rule

To deactivate an alarm rule, which will prevent notifications from being triggered for this rule until it is reactivated, click the **Deactivate** link, which appears in the last column of the rule.



Mute Alarms

From the **Mute Alarms** tab, you can suspend notifications for specific alarms on specific servers for a configured period of time. You can also see which alarms for which servers are currently muted.



To mute an alarm, perform the following steps:

Procedure

Step 1 From the **Alarm Names** drop-down list, choose the alarm that you want to mute. You can choose multiple alarms if needed. To select additional alarms, click in the **Alarm Names** field and the Alarm Names drop-down list will appear again allowing you to select an additional alarm.

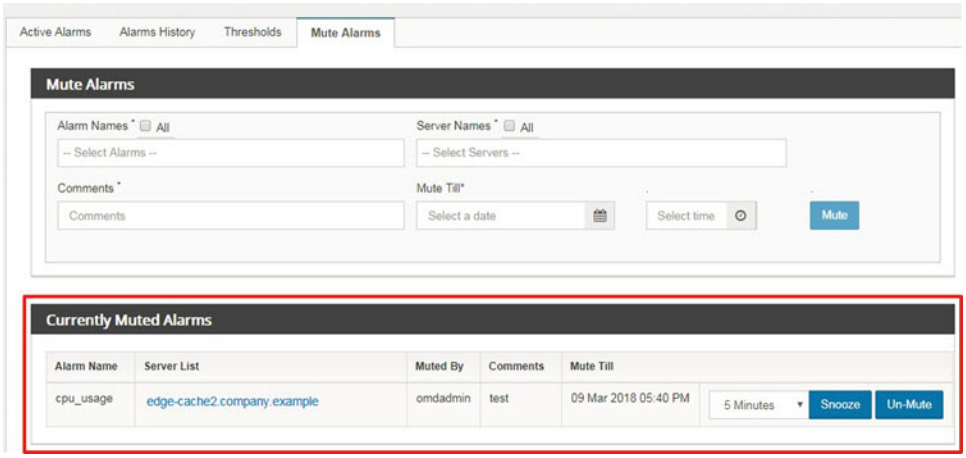
Step 2 From the **Server Names** drop-down list, choose the server for which you want to mute the alarm. You can choose multiple servers if needed. To select additional servers, click in the **Server Name** field, and the **Server Names** drop-down list will appear again allowing you to select an additional server.

Step 3 Enter a description.

Step 4 In the **Mute Till** field, use the calendar and time icons to choose when notifications for the alarm should resume.

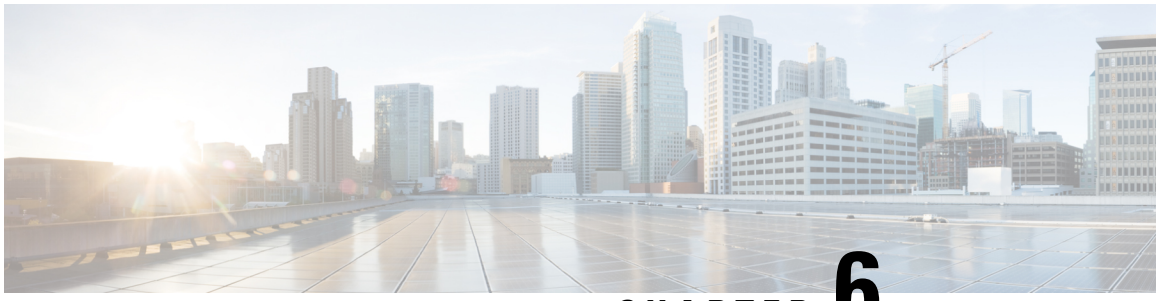
Step 5 When you are finished making changes, click **Mute** to mute the alarms.

Step 6 The muted alarms will now appear in the **Currently Muted Alarms** area.



From the Currently Muted Alarms section you can automatically unmute the alarm without waiting for the Mute Till date to be reached by clicking the **Un-Mute** button. You can also extend the Mute Till date by

clicking the **Snooze** button. This will extend the Mute Till date by the value selected in the time drop-down list that appears before the **Snooze** button.



CHAPTER 6

Media Broadcaster Insights

OMD Insights uses Splunk to provide deep analytics of the OMD Broadcaster environment that is based on mining statistics data from all Broadcaster servers. This enables OMD Insights to provide comprehensive OMD Broadcaster operational analytics, including analysis of throughput, utilization, and efficiency of multicasting delivery. It also provides insight into viewer trends. OMD Insights captures real-time data from Broadcaster statistic logs to provide simplified access to actionable data and analytics, so that operation teams can proactively monitor activity and take action before problems occur. It also delivers comprehensive dashboards and trending reports that capture valuable information for Broadcaster capacity planning and delivery optimization.

Note This guide only covers information as it pertains to Media Broadcaster. For other information on the additional features available from the Insights menu for a Media Streamer deployment, please see the *Cisco Media Streamer User Guide*.

This chapter includes the following sections:

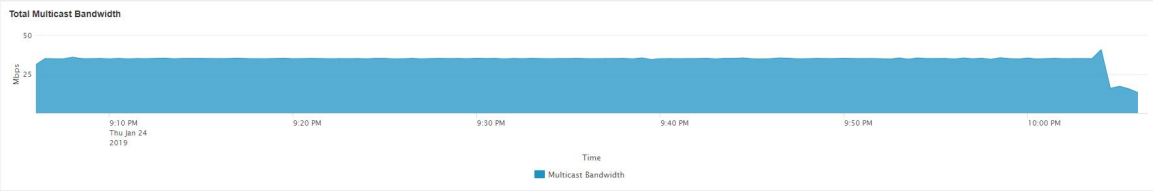
- Multicast Sending Charts, on page 65
- Multicast Receiving Charts, on page 67

Multicast Sending Charts

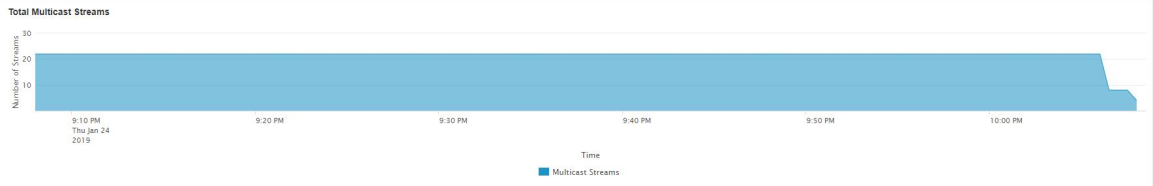
The charts located in OMD Director at **Media Broadcaster > Insights** on the Multicast Sending tab, show data related to various aspects of the Multicast Sending components within OMD. You can filter the data to only show charts for one specific MC-Sender or for all senders and you can filter charts by Channel and Representation ID. You can also change the Time Range, which forms the x axis of the graph, to show either the last 60 minutes, 4 hours, or 24-hour period. The following table displays the time intervals that the data is grouped and the time latency for receiving each data point. For example, if the time range is 60 minutes, the data is grouped in a 1 minute interval and you have to wait 3 minutes to receive a data point.

Time Range	Data Group Interval	Data Latency
60 minutes	1 minute	1 minute
4 hours	5 minutes	9 minutes
24 hours	5 minutes	9 minutes

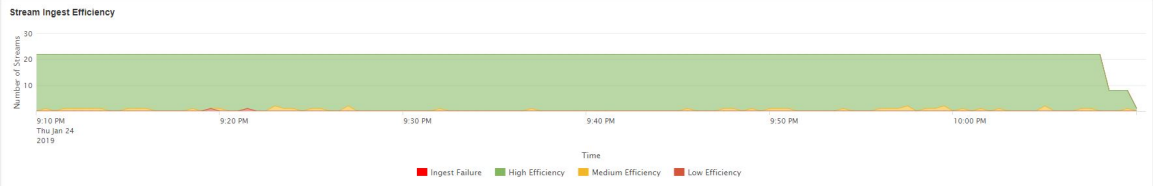
Total Multicast Bandwidth - shows the total amount of data multicasted by all MC-Senders, or for the selected MC-Sender, Channel, and Representation ID, as expressed in Mbps. The following is an example:



Total Multicast Streams – shows the total number of multicasted streams by all MC-Senders, or for the selected MC-Sender, Channel, and Representation ID. The following is an example:



Stream Ingest Efficiency – shows how efficiently MC-Senders are ingesting segments from the CDN or Origin Server. The following is an example:

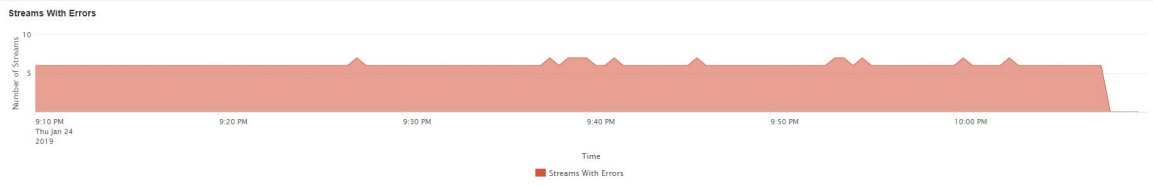


Stream ingest efficiency is calculated as a ratio of the segment fetch time divided by the segment length. Lower stream ingest efficiency numbers mean it takes less time on average to ingest the stream, providing higher (better) stream ingest efficiency. Ingest efficiency is denoted as one of the following:

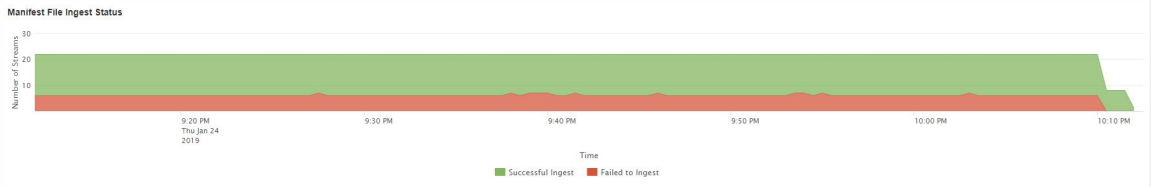
- Low efficiency: Streams that have a stream ingest efficiency value > 10%
- Medium efficiency: Streams that have a stream ingest efficiency value > 5% and <= 10%
- High efficiency: Streams that have a stream ingest efficiency value > .002% and <= 5%

The values used to determine low, medium, and high efficiency are hard-coded thresholds and cannot be changed. An Ingest Failure on a stream, or a stream that reports low efficiency, will trigger an alarm and will cause the MC-Receiver to start using a unicasting stream.

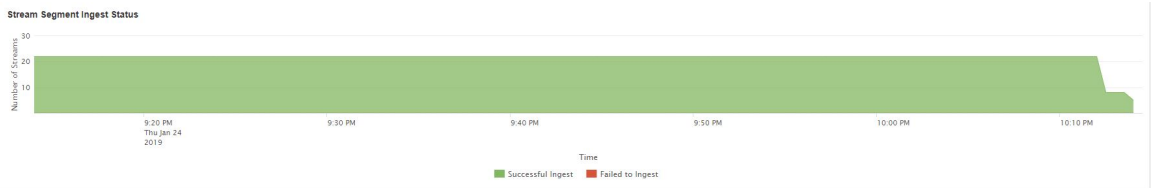
Streams with Errors - shows a count of MC-Sender streams that have experienced either a manifest file ingest failure, a segment ingest failure, or a segment multicast failure, along with the time at which those errors occurred. The following is an example:



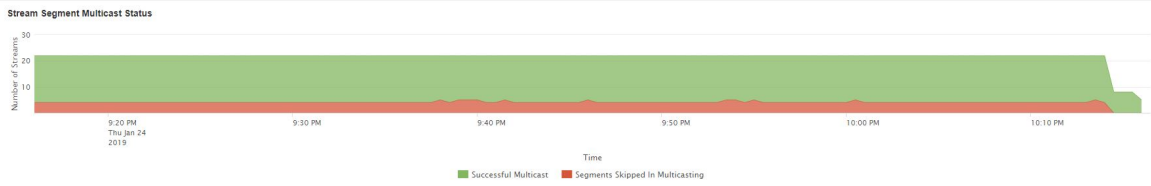
Manifest File Ingest Status - shows the number of streams for which the MC-Senders successfully ingested the manifest file (in green) or failed to ingest the manifest file (in red). Hovering your mouse over each data point or over the legend will indicate which specific channel(s) have succeeded or failed. The following is an example:



Stream Segment Ingest Status - shows the number of channels for which the MC-Senders have successfully ingested segments (in green) or failed to ingest segments (in red). Hovering your mouse over each data point or over the legend will indicate which specific stream(s) have succeeded or failed. The following is an example:



Stream Segment Multicast Status – shows the total number of multicasted stream segment successes and errors by all MC-Senders, or for the selected MC-Sender, Channel, and Representation ID. Multicasting errors are defined as streams with a segment skip or purge count that is greater than 0. When you click on a green or red data point, you will be taken to a screen that provides additional details. The following is an example:

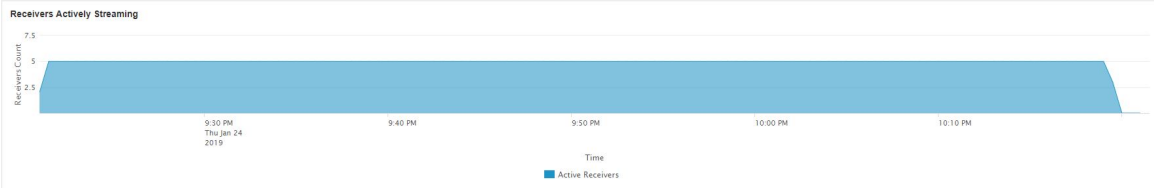


Multicast Receiving Charts

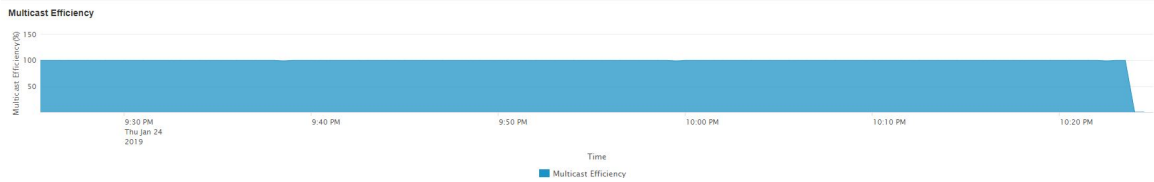
The charts located in OMD Director at **Media Broadcaster > Insights** on the Multicast Receiving tab, show data related to various aspects of all the Multicast Receiving components within OMD. You can filter charts by Channel, Representation ID, and Client ID. You can also change the Time Range, which forms the x axis of the graph, to show either the last 60 minutes, 4 hours, or 24 hour period. The following table displays the time intervals that the data is grouped and the time latency for receiving each data point. For example, if the time range is 60 minutes, the data is grouped in a 1 minute interval and you have to wait 5 minutes to receive a data point.

Time Range	Data Group Interval	Data Latency
60 minutes	1 minute	1 minute
4 hours	5 minutes	14 minutes
24 hours	30 minutes	59 minutes

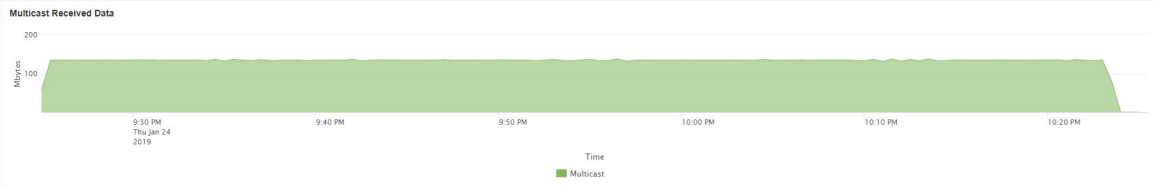
Receivers Actively Streaming - shows the total number of MC-Receivers that are actively receiving streams. The following is an example:



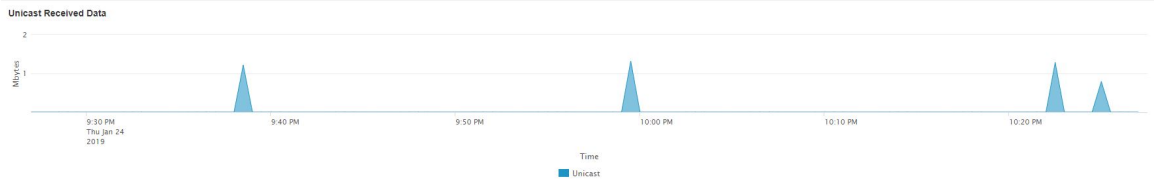
Multicast Efficiency – shows the percentage of the total multicast and unicast bytes received by the MC-Receivers that were multicast. This is an average across all MC-Receivers. The following is an example:



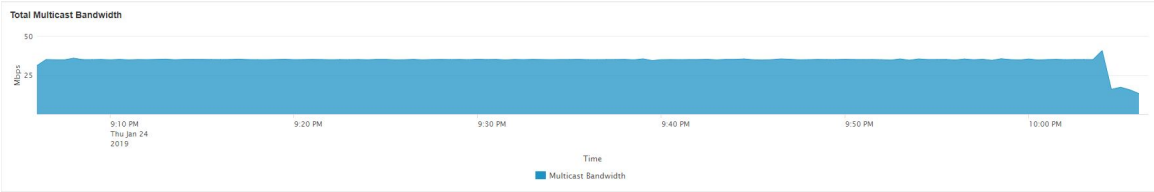
Multicast Received Data – shows the multicast data (in MB) that was received by all MC-Receivers from the MC-Senders. The following is an example:



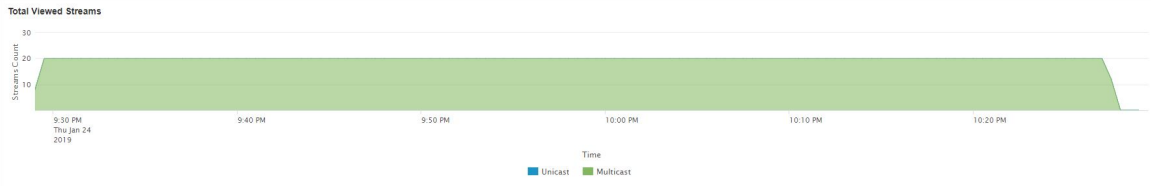
Unicast Received Data – shows the unicast data (in MB) that was received by all MC-Receivers from the CDN. The following is an example:



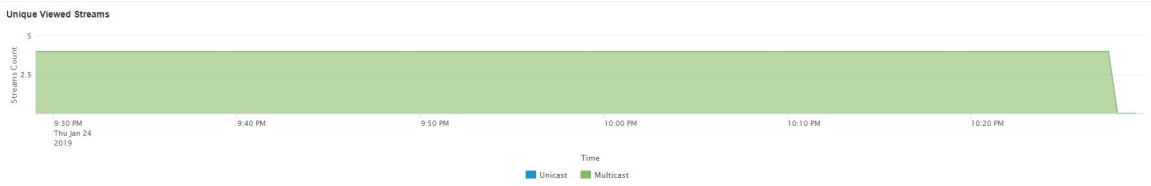
Error Correction Data - shows missing data (in MB) due to network transmission errors. That data is either repaired using the Forward Error Correction (FEC) data, unicast repair data, or it might remain unrepaired. Hover over the "FEC Repair", "Unicast Repair", or "Unrepaired" images in the legend to view the respective data for each. The following is an example:

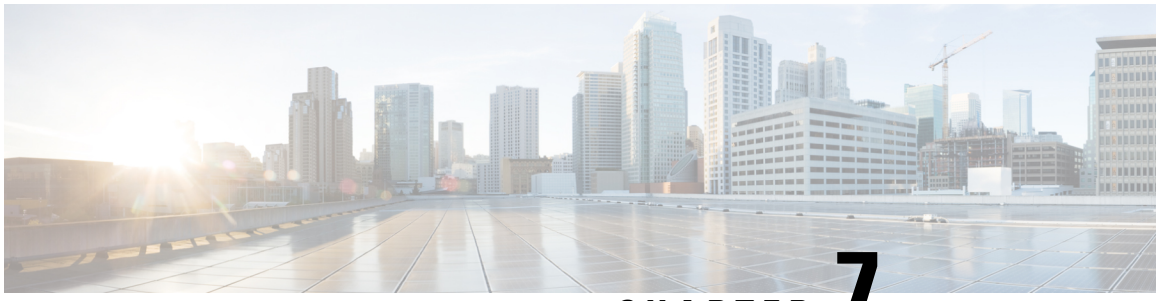


Total Viewed Streams – shows the total number of streams that was received by the MC-Receivers in either Unicast or Multicast mode. Hover over the Unicast or Multicast images in the legend to view the respective data for each. The following is an example:



Unique Viewed Streams – shows you the unique number of streams being received by the MC-Receivers in either Unicast or Multicast mode. If multiple customers are viewing the same stream, for example, then that will only count as one unique stream. Hover over the Unicast or Multicast images in the legend to view the respective data for each. The following is an example:





CHAPTER 7

OMD Director Administration

The **Administration** menu enables you to perform the following administrative tasks for Media Broadcaster:

- Manage the users who have access to OMD Director, including their privileges, and reset their passphrase.
- Manage the backups of the OMD databases, including adding remote backup destinations.
- Display an activity log that shows both user authentication and authorization activity, and CDN configuration activity.

This chapter also describes how to change the user settings for your account in OMD Director, including how to change your passphrase, how to configure what alarms you would like to receive notifications for, and how you would like to receive those notifications.

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this chapter, make sure you are logging into the Primary OMD Director instance. If you are logged into an OMD Director instance that is running in Backup mode, the header of the window will show "This OMD Director is currently running in backup mode". If you are logged into an OMD Director running in a detached state because of an HA failure, the header will show "This OMD Director is currently running in detached mode".

Note You must be logged in as a user with the Administrator role to access the **Administration** menu.

This chapter includes the following sections:

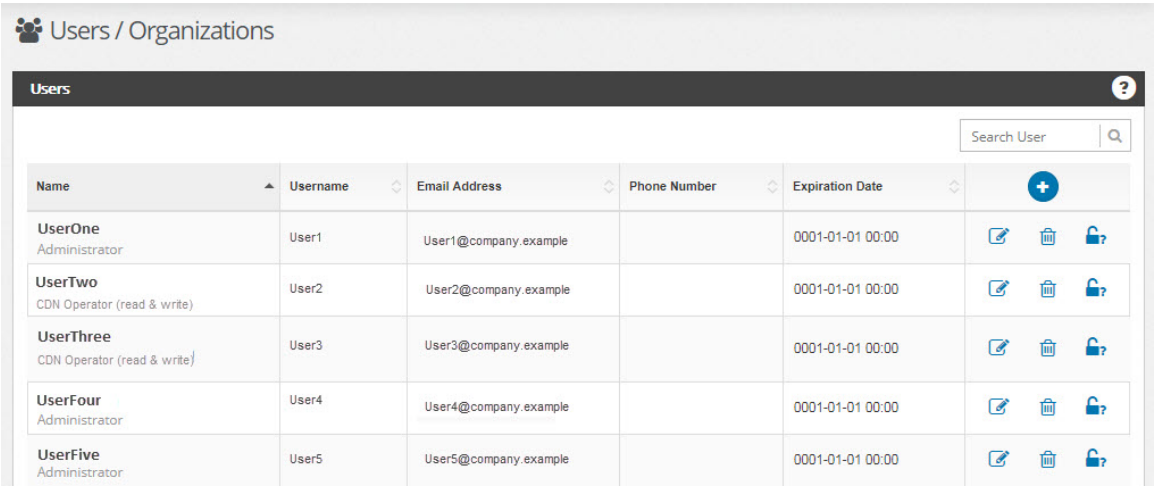
- Users/Organizations, on page 71
- Backup Management, on page 78
- User Profile, on page 84
- Activity Log, on page 88

Users/Organizations

When you choose **Administration** > **Users/Organizations** from the navigation panel, the Users/Organizations page appears. From this page you can do the following:

- View user information
- Add a new user
- Edit an existing user
- Delete a user
- Reset a user passphrase

Note Organizations are used for Media Streamer only.



The top area of the Users/Organizations page displays a list of users and the bottom area of the page displays a list of organizations that have been assigned to users and what users have been assigned to them.

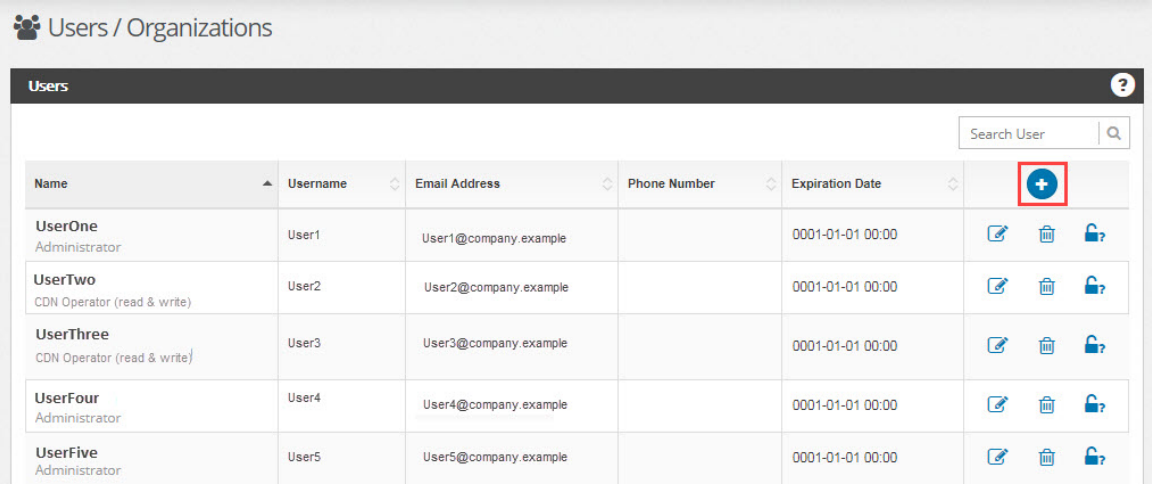
Add a New User

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this section, make sure you are logging into the Primary OMD Director instance.

To create a new user, perform the following steps:

Procedure

Step 1 From the Users section of the Users/Organizations page, in the header of the right most column, click the blue + icon.



Step 2 The Create New User window appears. Enter the following information for the new user:

- **Name:**
  - **First:** Enter the first name for the user. This is a required field and can only contain letters, spaces, and dashes (-).
  - **Middle:** Optionally enter a middle name. This field can only contain letters, spaces, and dashes (-).
  - **Last:** Optionally enter a last name. This field can only contain letters, spaces, and dashes (-).

  Note The user can change these fields.

- **Username:** Enter a username for the user. The username is what the user uses to log in to OMD Director. The username is case sensitive, must be at least 5 characters long, and can only contain letters and numbers. This is a required field.
- **Role:** Choose **Administrator**. Only users that are assigned a role of Administrator will be able to access the Media Broadcaster menus. Those users can also perform all of the functions available from all of the OMD Director menus, including creating and managing users.

  Note All of the roles other than Administrator apply only to Media Streamer.

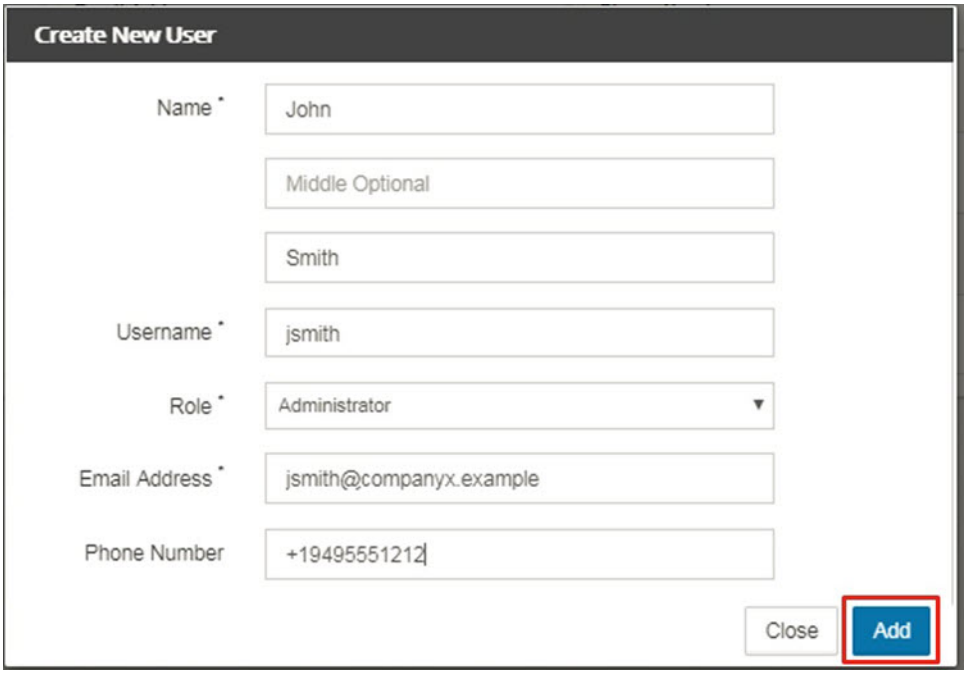
- **Organization:** This setting is used for Media Streamer. You can leave this field blank for Media Broadcaster users.
- **Email Address:** Enter the email address for the client. This is a required field.
  - If you have assigned an SMTP server to be used with OMD Director, this must be a valid email address for the user. This email address is used to send the user a temporary passphrase for their initial login. When the user logs in for the first time using this temporary passphrase, they will be prompted to change their passphrase. This email address is also used for notifications that the user configures if the user chooses Email as a Notify Through option.
  - If you have not assigned an SMTP server to be used with OMD Director, you can enter any email address as long as it is in the format user@server.com. In this case, after you create the user, the temporary password for the user will display on the screen. You will need to provide this password to the user.

Note The user can change this field.

- **Phone Number:** Optionally enter a phone number for the user. This phone number is also used for notifications that the user configures if the user chooses SMS as a Notify Through option.

  Note The user can change this field.

Step 3 Click **Add** to add the new user.



Step 4 If the user is created successfully, you will receive a confirmation message at the top of the Create New User window.

- If you have assigned an SMTP server to be used with OMD Director, the user will be sent an email with a temporary passphrase. This temporary passphrase is used the first time they log in to OMD Director. Upon their first log in, they will be prompted to change this temporary passphrase. The temporary passphrase expires 72 hours after it was created.
- If you have not assigned an SMTP server to be used with OMD Director, the temporary password for the user will display on the screen. You will need to provide this password to the user.

Step 5 Click **Close** to close this window, or repeat Step 2 and Step 3 to add another user.

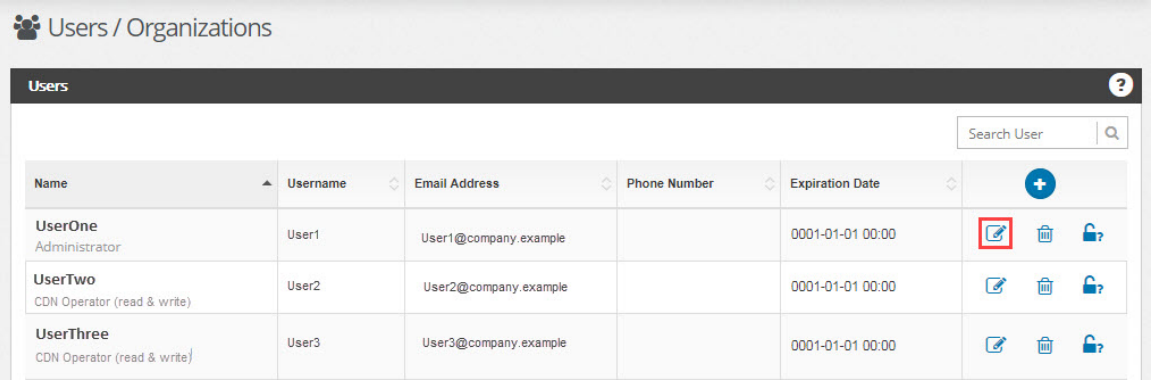
Edit an Exiting User

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this section, make sure you are logging into the Primary OMD Director instance.

To edit an exiting user, perform the following steps:

Procedure

Step 1 From the Users section of the Users/Organizations page, click the edit icon in the row of the user you want to edit.



Step 2 The Edit User window appears. Update the desired fields. You can change the following fields for the user:

- First name
- Middle name
- Last name
- Role

  Note If the user currently has the role of Content Provider (Admin) or Content Provider (Viewer), you cannot change their role or the Organization they have been assigned. If you need to change either of these values for a user, you must delete the user and recreate them.

- Email address
- Phone number

Step 3 When you are finished making your changes, click **Save**. If you want to exit the Edit User window without saving the changes, click **Close**.

Step 4 After you save the changes, a confirmation message appears at the top of the Edit User window. Click **Close** to close this window.

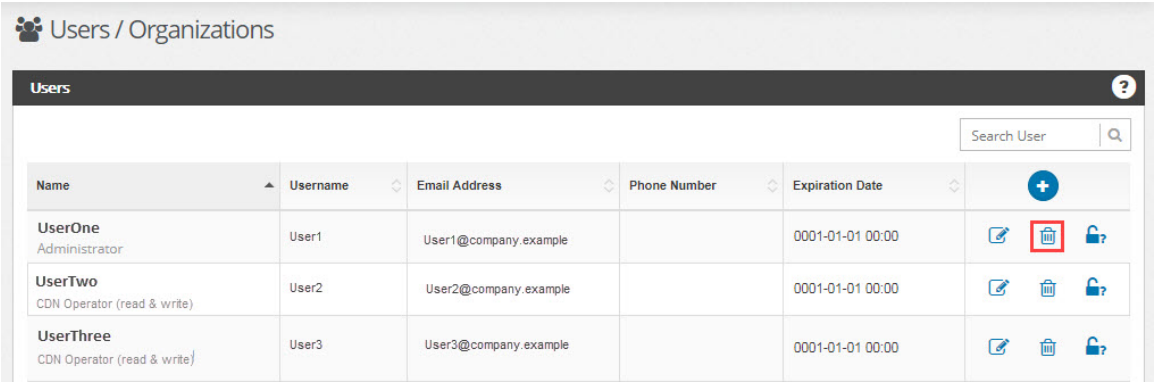
Delete a User

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this section, make sure you are logging into the Primary OMD Director instance.

To delete a user, perform the following steps:

Procedure

Step 1 From the Users section of the Users/Organizations page, click the delete icon in the row of the user you want to delete.



Step 2 The Delete User confirmation window appears. To finish deleting the user, click **Yes**.

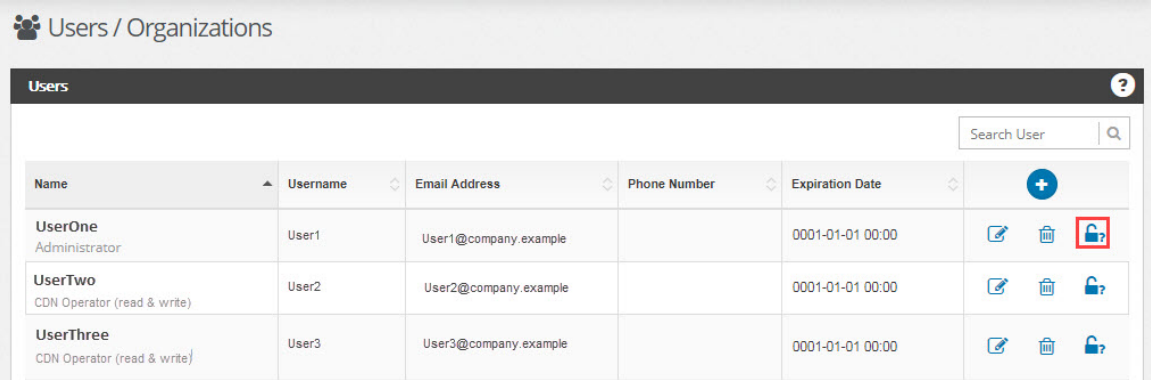
Reset a User Passphrase

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this section, make sure you are logging into the Primary OMD Director instance.

To reset the passphrase for a user, perform the following steps:

Procedure

Step 1 From the Users area of the Users/Organizations page, click the reset passphrase icon (the lock with the question mark) in the row of the user whose passphrase you need to reset. Clicking this link will reset the user passphrase to a temporary passphrase.



Step 2 After you click the reset passphrase icon:

- If you have assigned an SMTP server to be used with OMD Director, you will receive the message “Passphrase has been emailed successfully for username”. This indicates that the user passphrase has been successfully reset to a temporary passphrase and an email has been sent to the user. The email will direct the user to log in to OMD Director to change their passphrase. They will have 72 hours to do this before the temporary passphrase expires.
- If you have not assigned an SMTP server to be used with OMD Director, you will receive the message "Reset Passphrase Successfully" and the new temporary password will display on the screen. You will need to provide this password to the user.

Backup Management

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this section, make sure you are logging into the Primary OMD Director instance.

When you install OMD Director, it automatically schedules local daily backups of the databases that are managed by the OMD Director Worker node. These backups are saved in the `/home/ocdn_adm/director/backup_ms/backup_files/` folder on the OMD Director Worker node. You can also configure OMD Director to copy these backups to a remote server, which is recommended for disaster recovery, and you can change the frequency and day on which the backups occur. To configure these items and additional backup management features, go to **Administration** > **Backup Management**.

From the Backup Management window in OMD Director you can do the following:

- View a list of scheduled backups
- Change the frequency and time of a scheduled backup
- Enable or disable a scheduled backup
- Perform a backup or restore of a database
- Add remote backup destinations
- Modify remote backup destinations
- Add additional databases to back up
- Modify the settings for the databases that are already configured for back up

This section will cover how to perform these functions.

Schedule Backups

By default OMD Director is configured to perform a daily backup of the following OMD Director databases:

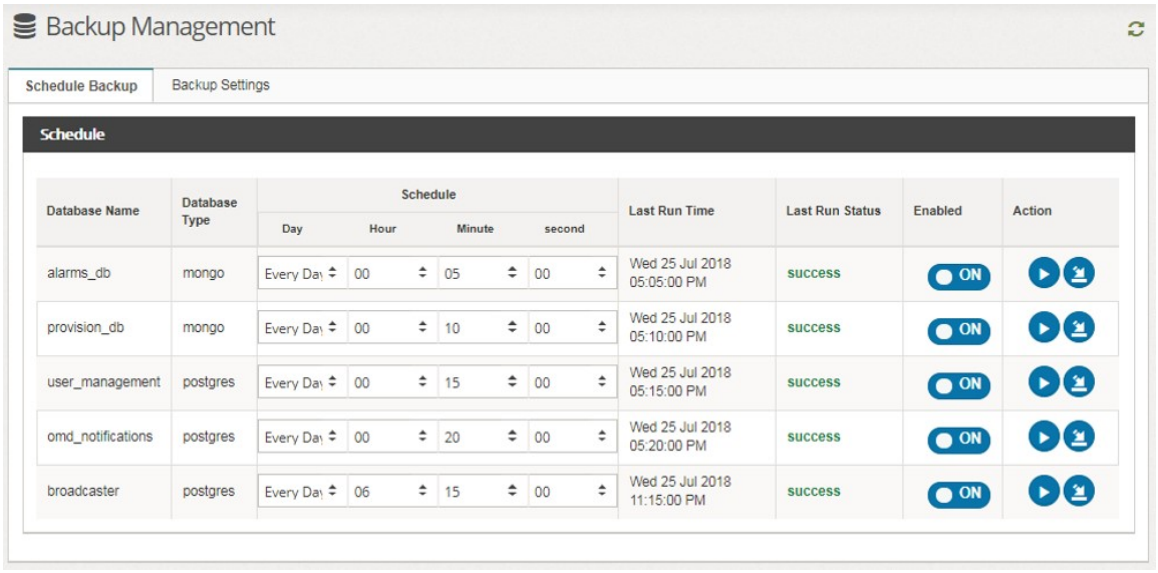
- alarms_db
- provision_db (this database is used for Media Streamer)
- user_management
- omd_notifcations
- broadcaster

You can see a list of the scheduled backups and make changes to when they occur from the Schedule page. To access the Schedule page, from the Backup Management window click the **Schedule Backup** tab. The Schedule page appears showing a list of databases to be backed up, the day and time they will be backed up, and whether the scheduled backup is enabled.

From the Schedule page you can do the following:

- Change the frequency and time of the backup for each database
- Enable or disable the scheduled backup
- Manually back up of a database
- Restore a database

The following is an example of a list of scheduled database backups:

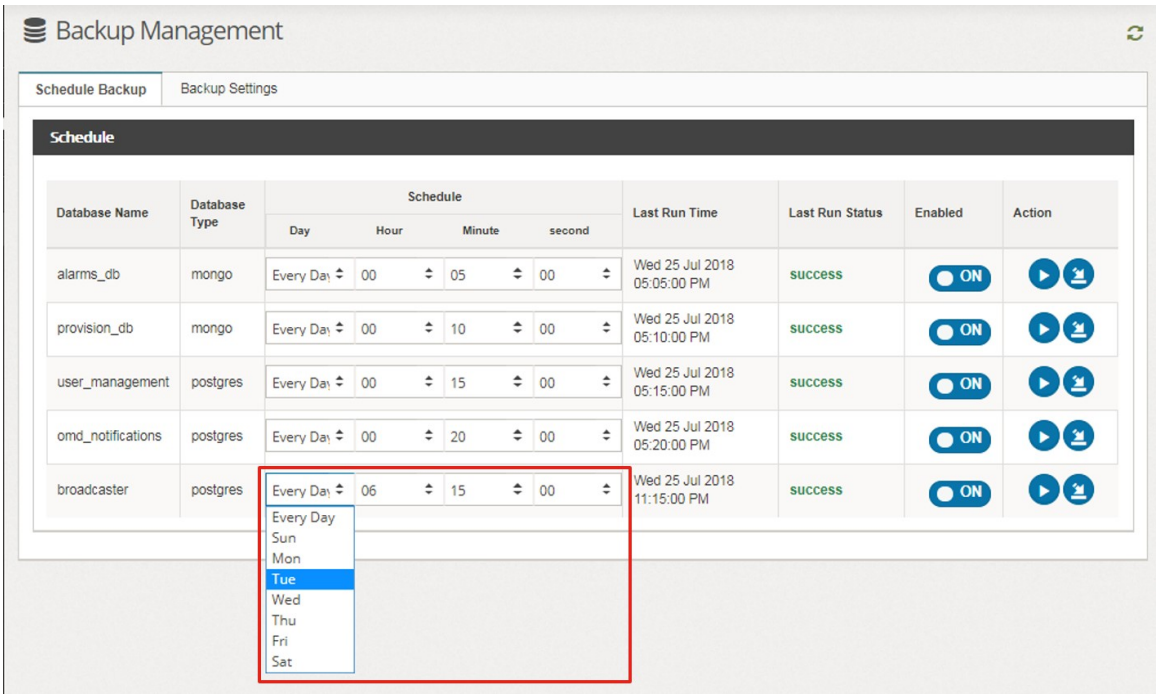


Change Schedule

The following is the default schedule for each database:

- **alarms_db:** Every day at 5 minutes after midnight
- **provision_db:** Every day at 10 minutes after midnight
- **user_managment:** Every day at 15 minutes after midnight
- **omd_notifications:** Every day at 20 minutes after midnight
- **broadcaster:** Every day at 6:15 am

To back up the database only once a week instead of daily, from the **Day** drop-down list, choose the day of the week to back up the database. To change the time of day that the backup should occur, choose the new time that you want from the Hour, Minute, and Second drop-down lists as appropriate.



Enable/Disable a Scheduled Backup

To disable the scheduled backup of a database, in the Enabled column of the database, slide the button to the right until you see “OFF”. To enable the scheduled backup, slide the button to the left until you see “ON”.

By default, the automatically created scheduled backups are enabled.

Manually Back Up and Restore a Database

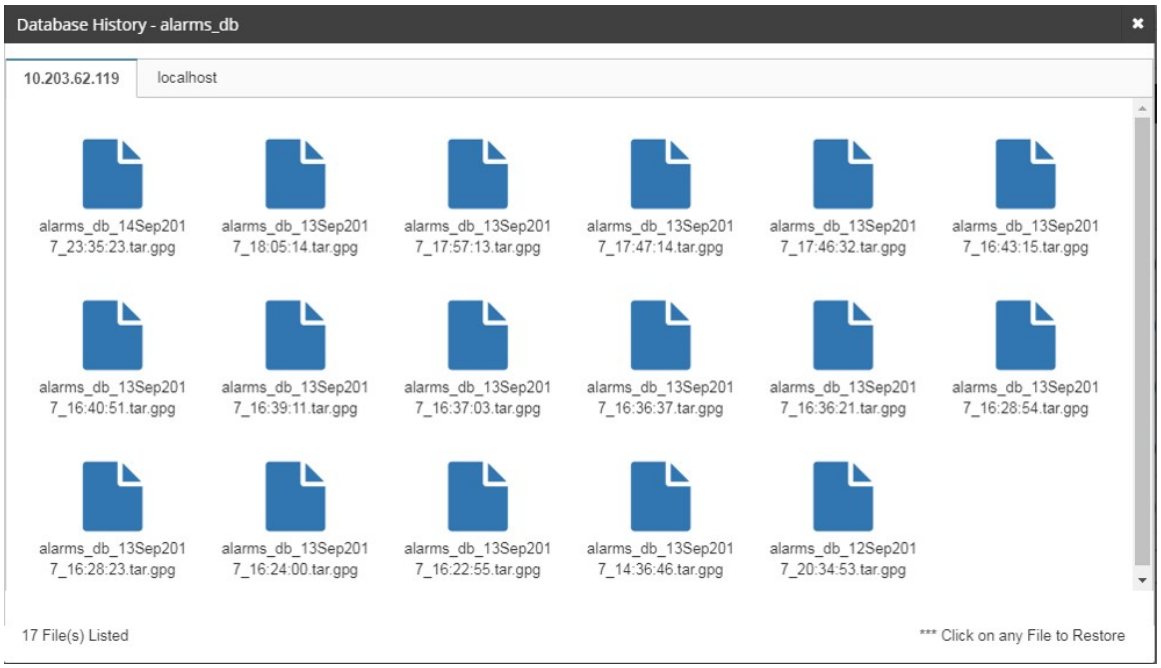
To perform a manual back up of a database, in the Action column of the database, click the **Backup Now** icon ( ). If the backup is successful, you will receive a backup completed message. This will create a copy of the backup locally on the OMD Director Worker node and on each remote server that has been configured. By default, there are no remote servers configured.

To restore a database from a backup file, perform the following steps:

Procedure

Step 1 In the Actions column of the database, click the **Restore** icon ( ). The Database History window appears. This window will have a localhost tab and a tab for every remote destination that is configured.

Note For the local copy of the backup, only the most recent successful backup is saved, so you will only have one file to choose on the localhost tab. For the remote copies of the backup, each successful backup that is run for a database will create a new file, so you will have multiple versions to choose from. The filenames will contain the date and time that the file was created to help you choose.



Step 2 Click the tab for the location that contains the backup file that you want to restore and then click the file to restore.

Step 3 When prompted, click **Yes** to confirm that you want to restore the database. If the restore is successful, you will receive a restore successful message.

Backup Settings

The Backup Settings tab contains two sections:

- **Backup Destinations:** By default the OMD Director databases are backed up locally to the `/home/ocdn_adm/director/backup_ms/backup_files/` folder on the OMD Director Worker node. It is also recommended that you configure OMD Director to copy these backups to a remote server for disaster recovery. From the Backup Destinations section you can add remote servers to copy the backup files to and you can test the connection to these servers.
- **Database Configuration:** From the Database Configuration section of the Backup Settings you can see information about the OMD Director databases that are currently being backed up and you can edit the settings for these databases. From this section you can also add additional Mongo or Postgres databases to back up. (The database must be on the OMD Director Worker node or a container on the OMD Director Worker node and you will need to provide the username and password for access.) Any databases that appear in the Database Configuration section will have a scheduled backup listed on the Schedule Backup tab.

Add Remote Backup Destinations

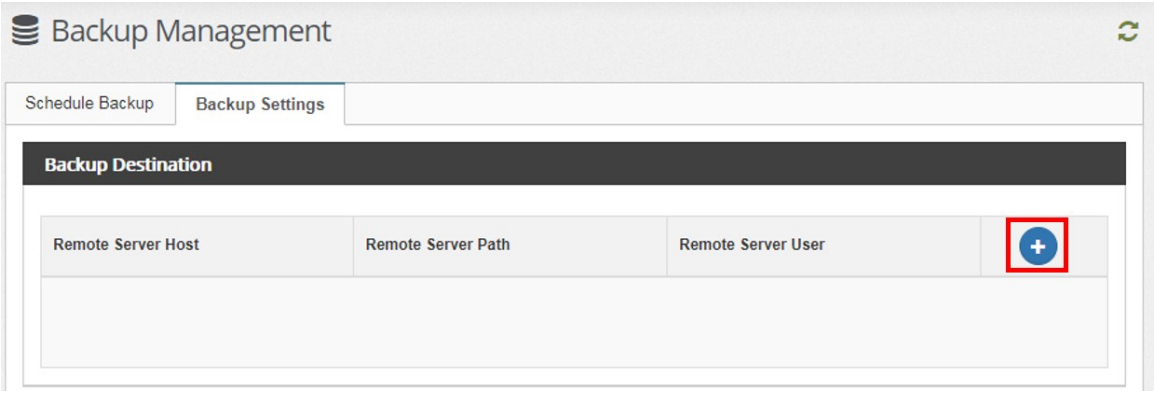
When you add a remote backup destination, every scheduled backup that is enabled in the Schedule list will save a copy of the backup file to the remote server, in addition to the local copy. For the local copy of the backup, only the most recent successful backup is saved. For the remote copies of the backup, each successful

backup that is run will create a new file; the filename will contain the date and time that the file was created. These files will be saved until you delete them. If you add multiple remote backup destinations, each destination will receive a copy of the database backup file for every scheduled backup.

To add a remote server as a database backup destination, perform the following steps:

Procedure

Step 1 From the **Backup Settings** tab in the **Backup Destination** area, click the Create New Destination (+) icon in the column heading of the last column.



Step 2 The Create Destination window appears. In this window, enter the values for the field as appropriate. The following table provides a description of the fields.

Table 3: Create Destination Fields

Fields	Description
Remote Server Host	Enter the IP address or hostname of the remote server
Remote Server Path	Enter the path on the remote server in which you want to save the database backups.
Remote Server User	Enter the username of a user that can SCP data to the server and that has access privileges to the Remote Server Path that is specified.
Private Key File	Browse for the private key file of the user you entered in the Remote Server User field.
Private Key Passcode	If the private key file requires a passcode, enter it in this field.

Step 3 Click **Add** to save the settings and add the new destination. You should receive a message that the destination was created successfully.

Step 4 After the remote server is added, click the Test Connection icon ( ) to confirm that you can connect to the server. You should receive the message that the destination was successfully verified.

Edit or Delete a Remote Backup Destination

To delete a remote backup destination, click the Delete icon ( ) for that destination. When prompted, click **Yes** to confirm the deletion of the backup destination.

To Edit the settings of a remote backup destination, click the Edit icon ( ) for that destination. The Edit Backup Destination page appears. Make the necessary changes to the settings, referring to Table 3: Create Destination Fields, on page 82 for a description of the fields. When you are finished making changes, click **Save**.

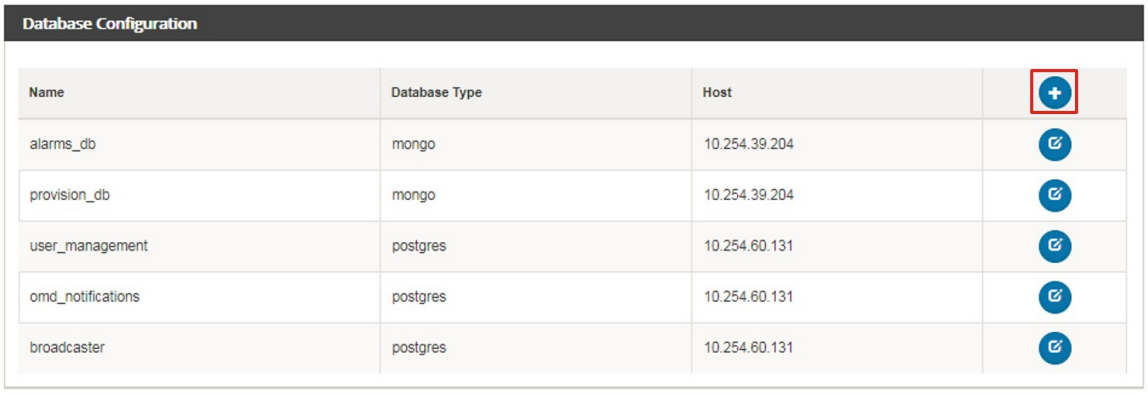
Add a New Database Backup

Note You can only add databases that are on the OMD Director Worker node or a container on the OMD Director Worker node.

To add a new Mongo or Postgres database to back up, perform the following steps:

Procedure

Step 1 From the Backup Settings tab in the Database Configuration section, click the Create New Database Backup (+) icon in the column heading of the last column.



Step 2 The Create New Database Backup window appears. In this window, enter the values for the field as appropriate. The following table provides a description of the fields.

Table 4: Create New Database Backup Fields

Fields	Description
Database Name	Enter the name of the database file to back up.
Database Type	Choose the type of database that is being backed up. The options are Mongo or Postgres.
Authentication Database	If the username that is used to log in to the database is not in the admin database, enter the authentication database for the user. **Note** This field is only for Mongo databases.
Host	Enter the IP address of the server that contains the database. This can be either the OMD Director Worker node or a container on the OMD Director Worker node.
Port	Enter the port number used to connect to the database. By default Mongo databases use 27017 and Postgres databases use 5432.
Username	Enter the username needed to log in to the database.
Password	Enter the password for the username that can log in to the database.

Step 3 Click **Add** to save the settings and add the new database configuration. You should receive a message that the database backup was created successfully.

Step 4 After the database configuration is added, an entry is automatically added to the Schedule list on the Schedule Backup tab. By default, the scheduled backup will be configured to run daily at midnight and will be disabled. Refer to Schedule Backups, on page 78 for details on changing these settings.

Edit a Database Configuration

To Edit the settings of a database configuration, click the Edit icon ( ) for that database. The Edit Database Configuration page appears. Make the necessary changes to the settings, referring to Add a New Database Backup, on page 83 for a description of the fields. When you are finished making changes, click **Save**.

User Profile

Note If you are running OMD Director in an HA configuration, you can only make configuration changes from the Primary OMD Director instance. To perform the steps in this section, make sure you are logged into the Primary OMD Director instance.

From the Profile page (in OMD Director), you can change the following information:

- Your first, middle, and last names
- Your email address
- Your phone number
- Your passphrase
- Your notification settings

Passphrase Criteria

Your passphrase must meet the following criteria:

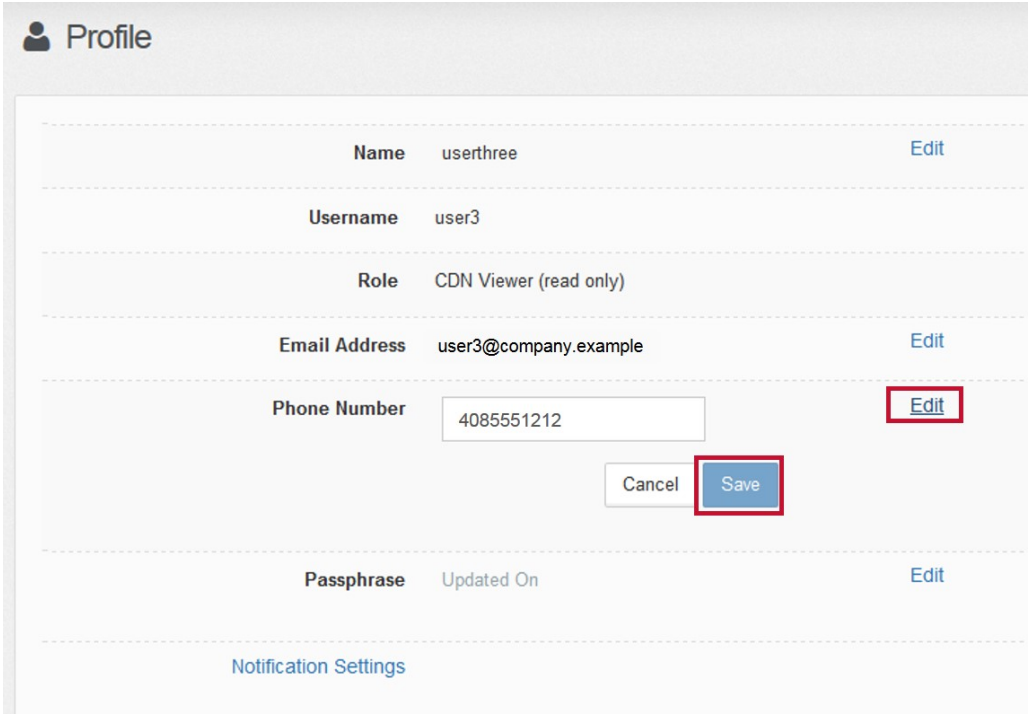
- By default, your passphrase must be at least 8 characters, but it should not exceed 47 characters. The default minimum length is configurable.
- Although these are configurable, by default, your passphrase must contain:
  - At least one letter
  - At least one number
  - At least one special character
- It cannot contain:
  - The following symbols or punctuation: €, @, #, " or ,
  - Any spaces (by default). This is configurable.

To access the Profile page to make changes, click your username and choose **Profile** on the upper-right side of the OMD Director window.

The Profile page appears.

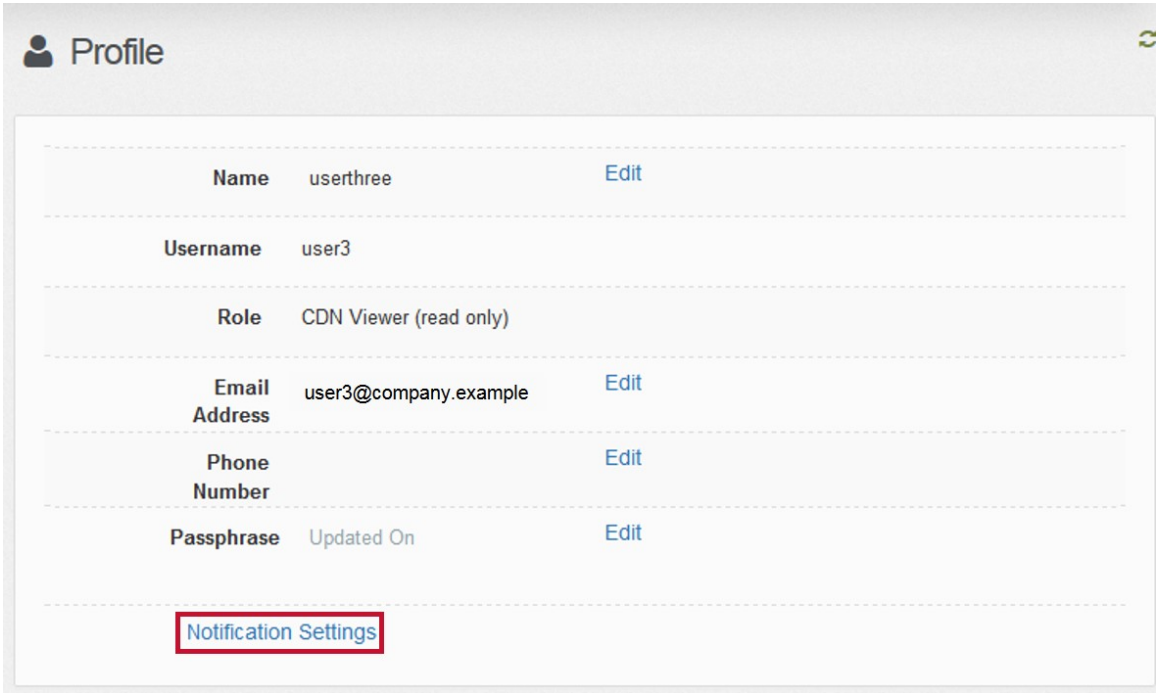
Change User Settings

To change your name, email address, or phone number click **Edit** next to the item that you want to change on the Profile page. When you have finished making any changes, click **Save**.



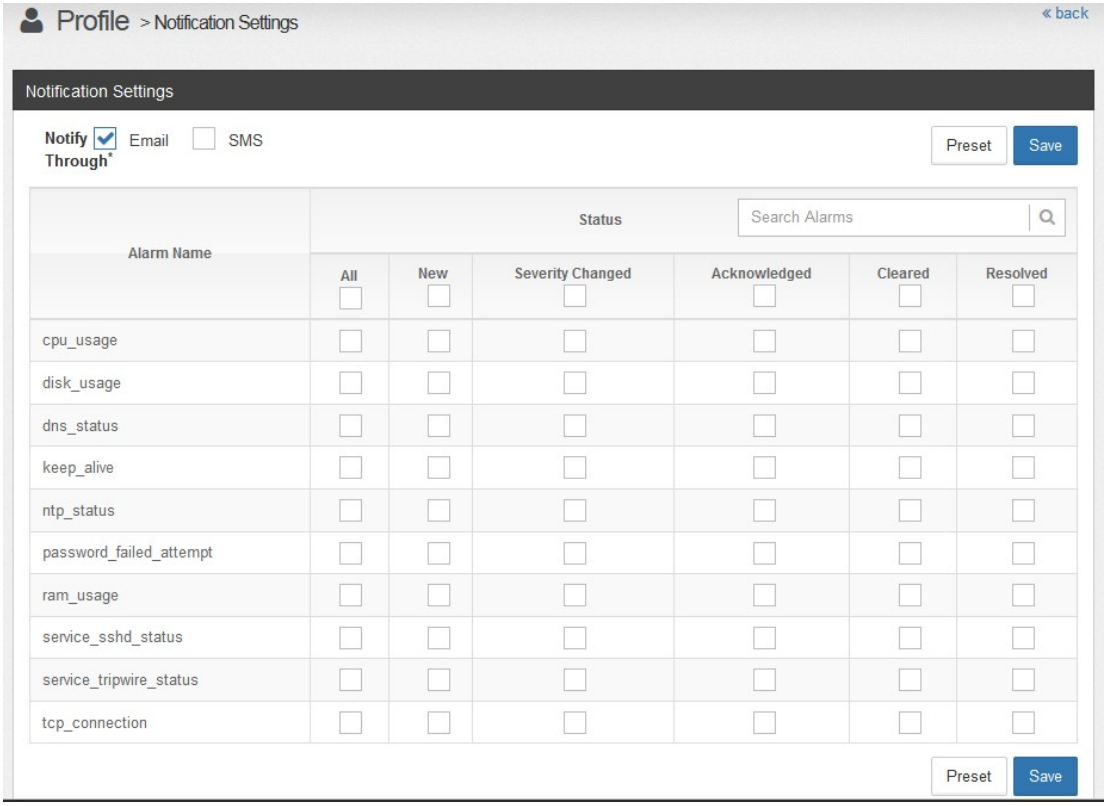
Notification Settings

From the Profile page you can configure your alarm notification settings. To access these settings, at the bottom of the Profile page, click the **Notification Settings** link.



The Notification Settings page appears. From this page you can configure which alarm names you would like to receive notifications for and what criteria for those alarms should trigger a notification. The criteria can be:

- If a new alarm is generated
- If the severity of an alarm has changed
- If an alarm is acknowledged
- If an alarm is cleared
- If an alarm is resolved



To choose which alarm names and which criteria for those alarms you would like to receive notifications for, you have the following options:

- Check the criteria check box for the individual alarm names for which you would like to generate notifications.
- To receive notifications for all of the alarm names for a specific criteria, check the check box in the column header for that criteria. For example, if you would like to receive a notification for any new alarms that are generated, regardless of what alarm name they are generated for, click the check box in the New column header.
- To receive notifications for all of the criteria for a specific alarm name, check the check box in the All column for that alarm name.

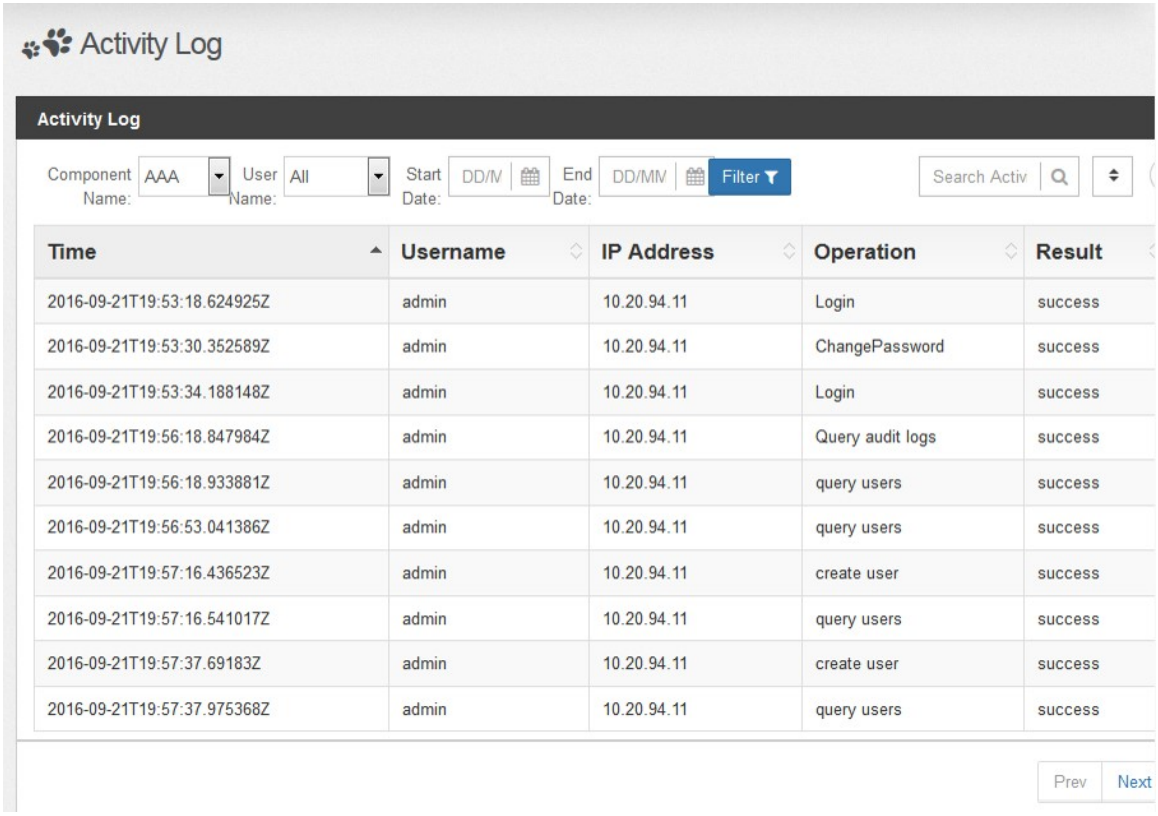
- If you would like to receive notifications for all of the criteria for all of the alarms, check the check box in the All column header. You can also use this check box to choose all of the alarms and then deselect the criteria for the alarms for which you do not want to receive notifications.

To actually receive the notifications, you must also configure whether you would like the notifications sent to you via email. To receive notifications via email, check the **Email check box** at the top left of the Notification Settings page. Email notifications are sent to the email address that is configured for your user account in OMD Director. If you need to change this setting, see Change User Settings, on page 85.

Note The SMS option is not supported in the current release.

Activity Log

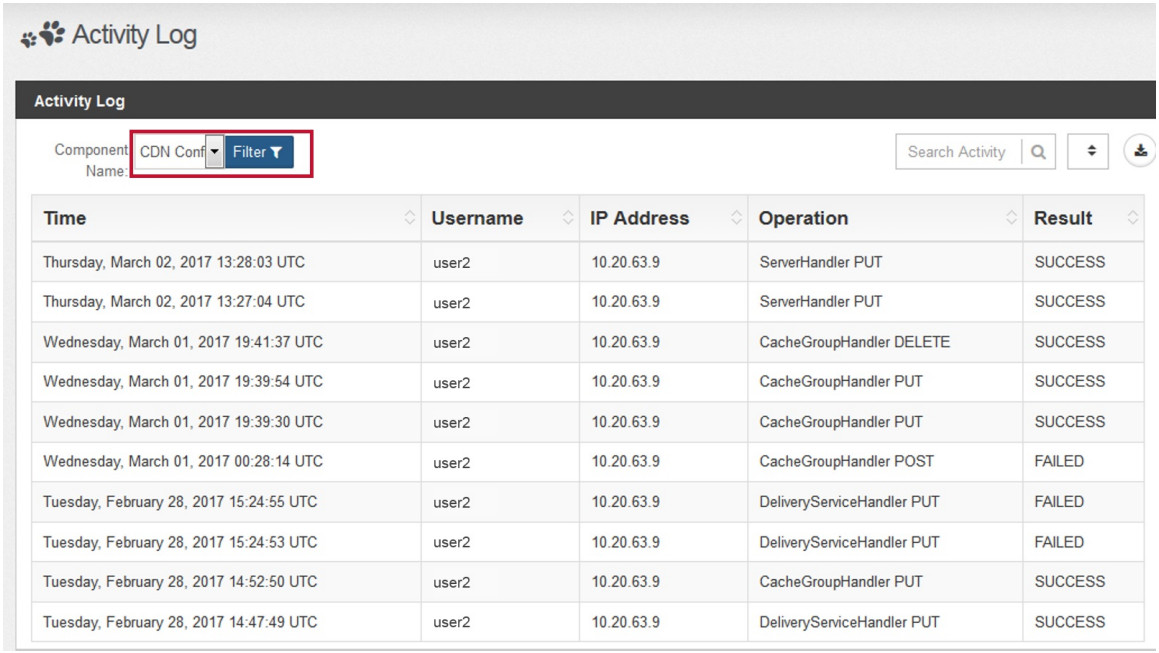
The Activity Log enables you to view an activity log that shows both user authentication and authorization activity, and CDN configuration activity. To access the Activity Log, choose **Administration** > **Activity Log** from the navigation panel.



The default page that appears displays the user authentication and authorization activity. From this page you can do the following for the AAA log entries:

- **Filter the information by user and date:** To filter the log entries based on these criteria, choose the user from the User drop-down list and optionally choose a Start Date and End Date. When you are done entering the filter criteria, click the **Filter** button.
- **Search the log entries:** To search the entries, enter the data you want to search for in the Search box. The text you enter is searched across all of the fields in the log entries.
- **Choose how many rows to display at a time:** You can choose this from the field next to the Search box. The options are 5, 10, 25, and 50. The default is 10.
- **Save the activity log as a JSON or CSV file:** To save the AAA activity to a file, click the download arrow at the end of the toolbar and choose the file format to save.

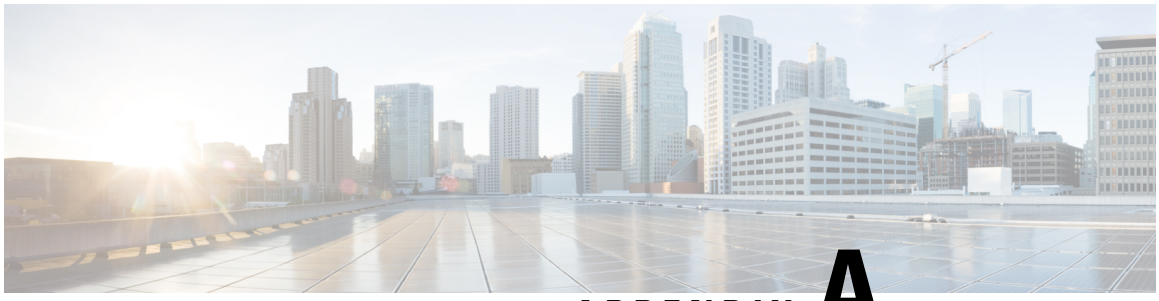
To view the CDN configuration activity, choose **CDN Configuration** from the **Component Name** drop-down list in the toolbar and click the **Filter** button.



Time	Username	IP Address	Operation	Result
Thursday, March 02, 2017 13:28:03 UTC	user2	10.20.63.9	ServerHandler PUT	SUCCESS
Thursday, March 02, 2017 13:27:04 UTC	user2	10.20.63.9	ServerHandler PUT	SUCCESS
Wednesday, March 01, 2017 19:41:37 UTC	user2	10.20.63.9	CacheGroupHandler DELETE	SUCCESS
Wednesday, March 01, 2017 19:39:54 UTC	user2	10.20.63.9	CacheGroupHandler PUT	SUCCESS
Wednesday, March 01, 2017 19:39:30 UTC	user2	10.20.63.9	CacheGroupHandler PUT	SUCCESS
Wednesday, March 01, 2017 00:28:14 UTC	user2	10.20.63.9	CacheGroupHandler POST	FAILED
Tuesday, February 28, 2017 15:24:55 UTC	user2	10.20.63.9	DeliveryServiceHandler PUT	FAILED
Tuesday, February 28, 2017 15:24:53 UTC	user2	10.20.63.9	DeliveryServiceHandler PUT	FAILED
Tuesday, February 28, 2017 14:52:50 UTC	user2	10.20.63.9	CacheGroupHandler PUT	SUCCESS
Tuesday, February 28, 2017 14:47:49 UTC	user2	10.20.63.9	DeliveryServiceHandler PUT	SUCCESS

From this page you can do the following for the CDN configuration log entries:

- **Search the log entries:** To search the entries, enter the data you want to search for in the Search box. The text you enter is searched across all of the fields in the log entries.
- **Choose how many rows to display at a time:** You can choose this from the field next to the Search box. The options are 5, 10, 25, and 50. The default is 10.
- **Save the activity log as a JSON or CSV file:** To save the AAA activity to a file, click the download arrow at the end of the toolbar and choose the file format to save.



APPENDIX A

Appendix: Cisco Media Broadcaster Log Files

This chapter provides information on the log file and stats file for the Multicast Controllers and Multicast Senders. These files can help you gather statistics for and troubleshoot the Media Broadcaster deployment.

- Log File Locations, on page 91
- Media Broadcaster Statistics: Multicast Receiver, on page 91
- Media Broadcaster Statistics: Multicast Sender, on page 92

Log File Locations

The log file for the Multicast Controller is located in the `/var/log/Broadcaster/MulticastController` directory.

All of the log files for the Multicast Sender are located in the `/var/log/Broadcaster/` directory:

- The log file for the MC-Sender interface is located in the `/var/log/Broadcaster/MulticastServerInterface` directory and is named msi.log.
- The log file for the multicast sender manager is located in the `/var/log/Broadcaster/MulticastSenderManager` directory and is named msm.log.
- The log files for the multicast sender application are located in the `/var/log/Broadcaster/MulticastSenderApplication` directory and all of the files end in .log. Each multicast sender application instance will have its own log file. The name of the log file will include the Source IP address for the multicast sender application instance.

Media Broadcaster Statistics: Multicast Receiver

Statistics are written to a log file on the Multicast Receiver and sent to the Multicast Controller, via a StreamStatus message. How often the Multicast Receivers of a broadcasting group send this information to the Multicast Controller is determined by the Stream Status Interval setting of the Multicast Receiver (also referred to as the Embedded Multicast Controller). By default this is 5 minutes. This information can help you gather statistics for and troubleshoot the Media Broadcaster deployment.

The MC-Controller stores the statistics it collects from the Multicast Receivers in the `/var/log/Broadcaster/MulticastController/ssr.log` file. This file contains the following fields:

- **id:** The device identifier of the Multicast Receiver

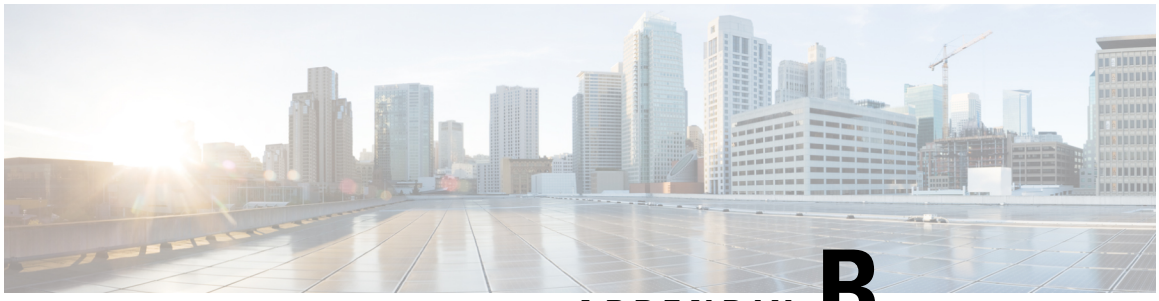
- **chn:** The stream being consumed by the player(s) behind Multicast Receiver
- **mcast:** The total number of bytes received from multicasting on the Multicast Receiver, including FEC parity symbol bytes and info message bytes
- **ucast:** The number of bytes received from unicasting on the Multicast Receiver
- **cH:** The number of bytes cached for the stream, including unicast
- **eF:** The number of bytes fixed by FEC
- **eR:** The number of bytes fixed with range request
- **eM:** The number of bytes that cannot be fixed by either FEC or range request
- **cMcast:** The actual bytes received via multicast that are written to the disk
- **format:** The video format, such as HLS or DASH
- **dState:** How the Multicast Receiver receives the stream when the message was sent

Media Broadcaster Statistics: Multicast Sender

The Multicast Sender Manager generates additional statistics in the `/var/log/Broadcaster/MulticastSenderManager/msm.log` file. This information can help you gather statistics for and troubleshoot the Media Broadcaster deployment.

This file contains the following fields:

- **url:** The stream currently being multicasted
- **bps:** The number of bytes being multicasted during this interval
- **ft:** How long it took to retrieve the last segment
- **p:** The number of segments purged
- **s:** The number of segments skipped
- **sf:** The number of segments that failed to be fetched
- **mf:** The number of manifest files that failed to be fetched
- **chn:** The channel name of the stream being ingested
- **repid:** The Representation ID of the channel being ingested



APPENDIX B

Cisco Media Broadcaster Troubleshooting

This section describes potential issues with Cisco Media Broadcaster and how to resolve them.

- Multicast Receiver Joins Multicast but no UDP Packets are Received at Socket Receive Buffers, on page 93
- Gateway does not Start the Multicast Receiver, on page 93
- Multicast Sender Unable to Acquire Content in a VPLS Network, on page 93

Multicast Receiver Joins Multicast but no UDP Packets are Received at Socket Receive Buffers

If you see multicast traffic at the interface level of the Multicast Receiver but do not see packets at the socket receive buffer, check whether the firewall is enabled. If the firewall is enabled, disable the firewall and check whether UDP packets arrive at the socket buffers.

Gateway does not Start the Multicast Receiver

If the gateway reports that it is still receiving unicast traffic for content, despite the multicast traffic being sent, it is possible that the gateway did not start the Multicast Receiver. A common cause of this is that the multicast URL Regex for the stream has not been correctly configured on the server. Check the configuration of this parameter in OMD Director (**Media Broadcaster > Broadcasting Groups**) to ensure that it correctly matches the URLs for the stream.

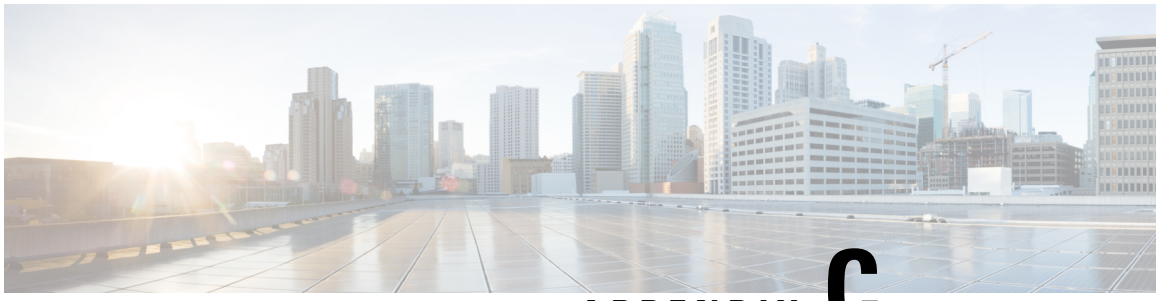
Multicast Sender Unable to Acquire Content in a VPLS Network

VPLS is a Layer 2 VPN technology that bridges Ethernet networks. For VPLS to work, it must add information in VLAN tags and MPLS tags in the IP packets. This can create an issue for the multicast sender that is trying to acquire content from the CDN when they are connected by a VPLS network in a star hub MPLS network overlay.

To diagnose an issue in a VPLS network, from the Multicast Sender, execute the following command:

```
ping -s 1472 do-not-fragment <dest-ip>
```

If you are unable to ping with a packet size of 1472 bytes (which is equal to 1500 bytes minus the IP header), then your MTU is too low. If you control the MPLS transport network, increase the MTU on the transit interfaces to make sure it accounts for the IP MTU plus VLAN headers and MPLS labels. To be safe, you could set all of the physical MTUs in the core network to 9100 bytes so that it is less likely that you will encounter an MTU problem. All of the edge-facing ports are set to the default MTU.



APPENDIX C

Appendix: OMD Director Alarms and Remediation

This Appendix describes the default checks and their thresholds that are run by the sensu-client service on the OMD Monitor clients that you can view and deactivate using OMD Director. To view these checks and their thresholds from OMD Director, choose **Monitor > Alarms** and click the **Alarm Rules** tab. This Appendix also describes possible remediation steps that you can perform if an alarm is raised.

When you triage the alerts that are raised, you should check the following items:

- Any active network configuration change requests that could affect traffic
- The active Media Broadcaster change requests for the servers in question
- Whether the alert indicates that end customer services are impacted
- Run the `dmesg | grep - i error` command and check for any errors
- Check the `/var/log/messages` files for any errors (grep -i error)

All notifications are generated based on the thresholds that are configured for the alarms. An alarm can have multiple thresholds configured for it to send notifications about different severity levels. To view the existing thresholds and to create new thresholds, from the **Monitor > Alarms** page, click the **Alarm Rules** tab. Table 5: Media Broadcaster Checks and Thresholds, on page 96 describes the default checks and thresholds that are available in OMD Director that are specific to Media Broadcaster components. Table 6: Common and OMD Monitor Checks and Thresholds, on page 100 describes the default checks and thresholds that are available in OMD Director that are common alerts or pertain to OMD Monitor. Table 7: Alarm Remediation Steps, on page 108 describes possible remediation steps you can perform based on the alarms or alerts that are raised.

The sections within this appendix are as follows:

- Media Broadcaster Checks and Thresholds, on page 96
- Common and OMD Monitor Checks and Thresholds, on page 100
- Media Broadcaster Alarm Remediation Steps, on page 108

Media Broadcaster Checks and Thresholds

Table 5: Media Broadcaster Checks and Thresholds

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]
bandwidth	mc-sender	Bandwidth usage on the MC-Sender in bps	**Warning:** Alert rasied if bandwidth is >= 1.8 Gbps **Critical:** Alert raised if bandwidth is >= 2 Gbps
broadcaster_config _manager	mc-controller	The status of the Broadcaster Configuration Manager component on the MC-Controller	**Critical:** Alert raised when the Broadcaster Configuration Manager is not operational
broadcaster_etcd	mc-controller	The status of the etcd service on the MC-Controller	**Critical:** Alert raised when the etcd service does not have a status of "Running"
broadcaster_haproxy	mc-controller	The status of the haproxy service on the MC-Controller	**Critical:** Alert raised when the haproxy service does not have a status of "Running"
broadcaster_keepalived	mc-controller	The status of the keepalived service on the MC-Controller	**Critical:** Alert raised when the keepalived service does not have a status of "Running"
broadcaster_ospfd	mc-sender	The running status of the ospfd service on the MC-Sender	**Critical:** Alert raised when the ospfd service does not have the status of “running”.
broadcaster_zebra	mc-sender	The running status of the zebra service on the MC-Sender	**Critical:** Alert raised when the zebra service does not have the status of “running”.

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]
failed_fetch_manifests	mc-sender	The number of manifest files that failed to be fetched from the origin server.	**Critical:** Alert raised if the number of manifest files that failed to be fetched from the origin server >=1
failed_fetch_segments	mc-sender	The number of segments that failed to be fetched from the origin server.	**Critical:** Alert raised if the number of segments that failed to be fetched from the origin server >=1
ingest_efficiency	mc-sender	Multicasting ingest efficiency is the ratio of the segment fetch time divided by the segment duration.	**Warning:** Alert raised if the multicasting ingest efficiency >=0.05 **Critical:** Alert raised if multicasting ingest efficiency >=0.1
multicast_control _manager	mc-controller	The status of the Multicast Controller Manager component on the MC-Controller	**Critical:** Alert raised when the Multicast Controller Manager is not operational
multicast_drops	mc-sender	The average multicast packet lost rate at the MC-receivers exceeds the configured threshold.	**Warning:** Alert raised if packet loss at MC-Receiver > 0.05 **Critical:** Alert raised if packet loss at MC-Receiver > 0.1
multicast_purge	mc-sender	The number of segments being purged during multicasting.	**Critical:** Alert raised if the number of segments being purged during multicasting >=1
multicast_sender _manager	mc-sender	The status of the Multicast Sender Manager component on the MC-Sender	**Critical:** Alert raised when the Multicast Sender Manager is not operational
multicast_server _interface	mc-sender	The status of the Multicast Server Interface component on the MC-Sender	**Critical:** Alert raised when the Multicast Server Interface is not operational

Appendix: OMD Director Alarms and Remediation

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]
multicast_skipped _segments	mc-sender	The number of segments being skipped during multicasting.	**Critical:** Alert raised if the number of segments being skipped during multicasting >=1
no_multicasting_streams	mc-sender	The number of MC-receivers failing to receive multicast streams exceeds the configured threshold.	**Warning:** Alert raised if no multicasting received at MC-Receiver >=0.05 **Critical:** Alert raised if no multicasting received at MC-Receiver >=0.1
streams_not_multicastable	mc-sender	The streams that are not multicastable exceeds the configured threshold. Typically, this occurs when the stream is not defined in the channel map, or when there are not enough MC-Receivers joining that channel to make it multicast.	**Warning:** Alert raised if the streams not multicastable >=0.2 **Critical:** Alert raised if the streams not multicastable >=0.5
stream_status_receiver	mc-controller	The status of the Stream Status Receiver component on the MC-Controller	**Critical:** Alert raised when the Stream Status Receiver is not operational
stream_status_messages _per_second	mc-controller	Number of stream status messages received per second	**Warning:** Alert raised if the number of stream status messages received is >= 1500 per second **Critical:** Alert raised if the number of stream status messages received is >= 1670 per second

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]
multicast_drops	mc-sender	Multicast packet loss at MC-Receiver exceeds the configured threshold	**Warning:** Alert raised if the number of stream status messages received is >= 0.05 per second **Critical:** Alert raised if the number of stream status messages received is >= 0.1 per second
no_multicasting _streams	mc-sender	No multicasting received at MC-Receiver exceeds the configured threshold	**Warning:** Alert raised if the number of stream status messages received is >= 0.05 per second **Critical:** Alert raised if the number of stream status messages received is >= 0.1 per second
streams_not _multicastable	mc-sender	Streams not multicastable exceeds the configured threshold	**Warning:** Alert raised if the number of stream status messages received is >= 0.2 per second **Critical:** Alert raised if the number of stream status messages received is >= 0.5 per second

Common and OMD Monitor Checks and Thresholds

Table 6: Common and OMD Monitor Checks and Thresholds

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
cpu_usage	common	CPU usage in percentage (0 - 100%)	Warning alarm raised if: • >= 50% (Default) • >= 80% (Monitor Node) Critical alarm raised if: • >= 80% (Default) • >= 95% (Monitor Node)	Warning: N/A Critical: P4
disk_usage	common	Total disk usage in percentage	Warning alarm raised if: • >= 85% (Default) • >= 90% (Monitor Node) Critical alarm raised if: • >= 95%	Warning: N/A Critical: P3/P4

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
dns_resolved_status	common	Status of DNS resolution: • 0: DNS is not resolvable • 1: DNS is resolvable	Critical: Alert raised if DNS is not resolvable (check result returns 0)	P4
hardware	common	Hardware error message status from the dmesg command output: • 0: No errors found • 1: Errors found	Warning: Alert raised if errors found (check result returns 1)	P3
influx_connectivity	common	Checks connectivity to OMD Monitor Influx nodes. • 0: Normal connectivity • 2: No connectivity to any OMD Monitor Influx nodes	Critical: Alert raised if none of the OMD Monitor Influx nodes are reachable.	P3
influx_metrics_not_found	common	0: Normal no errors found 2: Critical	Critical: Metrics not found from OMD Monitor Influx nodes at this time	
kafka_broker_status_all	monitor-node	The number of servers that are having a problem with the Kafka broker server. 0 means all servers are fine or there are no servers configured for Kafka export.	Critical: Alert raised if any or all Kafka brokers are not able to export metrics	P3/P4

Appendix: OMD Director Alarms and Remediation

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
keep_alive	common	The status of the Monitor node connection to the server node being monitored. To determine this, keepalives are sent by the sensu-client service on the server node to a Monitor node every 30 seconds: • 0: Not reachable • 1: Reachable	Warning: Alert raised if no keepalives have been received for 90 to 180 seconds Critical: Alert raised if no keepalives have been received for more than 180 seconds	P3/P2 The priority is determined based on the number of servers that are raising the keepalive. If a single server is in this state, it is a P3. If there is a block of servers that are affected, it is a P2 and you should escalate immediately.
load_avg_1min	common	CPU load average values, with regards to both the CPU and I/O over the last minute. This value is a decimal number and not a percentage. These values are taken from the /proc/loadavg system file.	Warning: Alert raised if load_avg_1min >= 10 Critical: Alert raised if load_avg_1min >= 25	Warning: N/A Critical: P4
load_avg_5min	common	CPU load average values, with regards to both the CPU and I/O over the last 5 minutes. This value is a decimal number and not a percentage. These values are taken from the /proc/loadavg system file.	Warning: Alert raised if load_avg_5min >= 20 Critical: Alert raised if load_avg_5min >= 50	Warning: N/A Critical: P4

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
log_failed_notallowed	common	The number of SSH failed login attempts due to access restrictions	Warning: Alert raised if 1 failed attempt Critical: Alert raised if 2 or more failed attempts	P4
log_failed_password	common	The number of failed login attempts do to incorrect passphrase	Warning: Alert raised if 1 failed attempt Critical: Alert raised if 2 or more failed attempts	P4
netstat	established	This check indicates the number of connections in the ESTABLISHED state. An alarm is raised if the number of connections exceeds the configured threshold. A server only has a finite number of TCP connections available, so this alarm indicates when the server is nearing that threshold. Connections are determined by looking for ESTABLISHED and TIME_WAIT entries using the netstat command.	Warning: Alert is raised if ESTABLISHED connections are at the following thresholds: • >= 500 (Default) • >= 1500 (monitor node) Critical: Alert is raised if ESTABLISHED connections are at the following thresholds: • >= 1000 (Default) • >= 2000 (monitor node)	Warning: N/A Critical: P4

Appendix: OMD Director Alarms and Remediation

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
netstat	time_wait	This check indicates the number of connections in the TIME_WAIT state. An alarm is raised if the number of connections exceeds the configured threshold. A server only has a finite number of TCP connections available, so this alarm indicates when the server is nearing that threshold. Connections are determined by looking for ESTABLISHED and TIME_WAIT entries using the netstat command.	Warning: Alert is raised if TIME_WAIT connections are: • >= 500 (Default) • >= 1500 (monitor node) Critical: Alert is raised if TIME_WAIT connections are: • >= 1000 (Default) • >= 2000 (monitor node)	Warning: N/A Critical: P4
ntp_sync_status	common	The status of the sync with the NTP server. 0 indicates the server is not in sync. 1 indicates the server is in sync.	Critical alarm raised if ntp_offset >= 500ms	Critical: P4

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
partition_usage	Name of each partition: /var /sys/fs/cgroup /run /opt /dev /dev/shm /boot /	Disk usage for each partition, as a percentage. This check will return 1(warning) if the configured warning or critical threshold values are more than 100.	Warning: Alert raised if any partition usage >= 85% Critical: Alert raised if any partition usage >= 95%	Warning: N/A Critical: P4
ram_usage	common	RAM usage as a percentage	Warning: Alert raised if RAM Usage is >= 80% Critical: Alert raised if RAM Usage is >= 95%	P4
redis_status	monitor-node	The number of connected OMD Monitor nodes. This number should be equal to the number of OMD Monitor nodes available at install. If it is not, a warning is raised.	Warning: Alert raised if the number of connected OMD Monitor nodes is less than the number of OMD Monitor nodes available at initial installation.	N/A
service_status	grafana-server	The running status of the Grafana server on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the grafana-server service does not have the status of “running”.	P4

Appendix: OMD Director Alarms and Remediation

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
service_status	haproxy	The running status of the haproxy service on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the haproxy service does not have the status of “running”.	P4
service_status	influxdb	The running status of the influxdb service on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the influxdb service does not have the status of “running”.	P4
service_status	influxdb-relay	The running status of the influxdb-relay service on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the influxdb-relay service does not have the status of “running”.	P4
service_status	rabbitmq-server	The running status of the rabbitmq-server service on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the rabbitmq-server service does not have the status of “running”.	P4/P3
service_status	redis	The running status of redis service on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the redis service does not have the status of “running”.	P4/P3

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
service_status	redis-sentinel	The running status of redis-sentinel service on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the redis-sentinel service does not have the status of "running".	P4/P3
service_status	sensu-server	The running status of sensu-server service on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the sensu-server service does not have the status of "running".	P4/P3
service_status	splunk	The running status of splunk service on the OMD Monitor node: • 0: Not running • 1: Running	Critical: Alert raised when the splunk service does not have the status of "running".	P4/P3
service_status_ rabbitmq-metrics-exporter	rabbitmq-metrics-exporter	Running status of rabbitmq-metrics-exporter on monitor node: • 0: Running • -1: Not Running	Critical when rabbitmq-metrics-exporter service is not in running state.	P2/P3
service_status_tcp -rabbitmq-exchange	tcp-rabbitmq-exchange	Running status of tcp-rabbitmq-exchange on monitor node: • 0: Running • -1: Not Running	Critical when tcp-rabbitmq-exchange service is not in running state.	P2/P3

Check Name	Entity Family (entity_family in Influxdb)	Check Value	Alarm Condition/ Check Result [0 - No Alert/Normal] [1 - Warning Alert] [2 - Critical Alert]	Severity/Priority
sshd_running_status	common	The running status of the sshd service: • 0: Not running • 1: Running	Warning: Alert raised if the sshd service is not running.	P4
swap_usage	common	The percentage of swap usage	Warning: Alert raised when swap usage is >= 95% Critical: Alert raised when swap usage is >= 98%	P2
tcp_connection	other	Number of TCP connections including TCP6	Warning: Alert raised if TCP connections are: • >= 500 (others) Critical: Alert raised if TCP connections are: • >= 1000 (others)	Warning: N/A Critical: P4
tripwire_violations	common	The number of tripwire report violations. Local local files are checked for changes.	Critical: If any tripwire violations are found (check result is 3)	P4

Media Broadcaster Alarm Remediation Steps

Table 7: Alarm Remediation Steps

Check	Remediation
bond_interface	If this alarm has been raised, the alarm should have already been cleared so a keepalive alarm should have been raised. Also look at the IPMI Interface check in Traffic Ops to see if the server has power.

Check	Remediation
cpu_usage	Level 3: • Check the running state of the system to determine if there is an issue. If the alert is generated and resolved immediately, it may be able to be ignored. • This may or may not be an issue depending on the load/traffic on the server. If the alert continuously persists, execute the **top** command on the client terminal to determine which process is running high on CPU. • Check the Grafana dashboard for any patterns in the usage.
disk_drives_count	Log in to the cache node and use the `ls /dev/sd*` command to check the disk drive partitions list. Based on the profile of Mid or Edge cache sever, the list will change. sda, sdb, sdc, and so on are the disk drives and sda1, sda2, and so on are partitions in sda. Check if any disk is missing based on the profile.
disk_usage	Level 2/Level3: For critical alerts, log in and check how different partitions are being used. Use the `df` command to determine which partitions have high disk usage.
dns_resolved_status	Level 1/Level 2: Make sure servers have access to DNS servers and that those DNS servers are correct.

Appendix: OMD Director Alarms and Remediation

Check	Remediation
hardware	Indicates a possible hardware error. Details can be found in the `/var/log/messages` file. The check is looking for "Hardware Error" in the `/var/log/messages log` file (using the `dmesg` command). Perform the following steps: Stash (mute) the alert while investigating the issue, otherwise the alert will repeat every 5 minutes. SSH to the affected system and change to the root user. Collect the relevant portion of the `/var/log/messages` file for information on the hardware error. Send an email for a case to be opened, including all of the collected information. See the note below Back up the dmesg log using the following command: `dmesg > /var/log/dmesg-`date +%Y%m%d_%I%M%S`` Enter the `dmesg -c` command to clear the dmesg log. Unstash (unmute) the alert. **Note** Level 1 should create a case with the hardware vendor and ask them to identify what the error means and to recommend the next steps. If the vendor recommends a DIMM replacement, ensure that the issue has actually been identified. Ask the vendor to explain why the DIMM needs to be replaced and to identify which slot is referenced in the error message.
influx_connectivity	Check whether there is a network event that is causing the loss of connectivity. If no possible cause can be found, escalate to Level 2 or Level 3.
insights_failover_check	Check the connectivity between the primary and backup OMD Insights nodes. There may be network connectivity issues between the primary and backup OMD Insights nodes that resulted in this alarm. Check for any keepalive alerts from OMD Monitor for the OMD Insights primary nodes.
interface	Level 2: Verify that the issues is not external to the CDN cache nodes and then escalate as needed.

Check	Remediation
kafka_broker_status_all	Check the accessibility of the Kafka servers from the OMD Monitor nodes: • Check the omd.conf pillar file on the Salt Master and verify the Kafka servers and their ports are configured correctly. • SSH to the OMD monitor node and verify connectivity to the Kafka servers. • Check the /var/log/sensu/sensu-server.log and /etc/sensu/kafka_broker_status.log log files for any error messages.
keep_alive	Network connectivity between an OMD Monitor node and the server being monitored might have been lost. Additional insight into the network is required. If you can access the server using SSH, you can run the following commands to determine whether the system rebooted or if there was a network issue: • **uptime:** This command shows how long the system has been up. If it has been up for well before the alert, than use the next command to further troubleshoot. • **grep "NIC Link" /var/log/messages*:** This will display the details for the interface status, if it had a problem. If neither of these commands reveal an issue, perform additional review of the following log files: • `/var/log/sensu/sensu-client.log` on the server • `/var/log/sensu/sensu-server.log` on Monitor nodes

Appendix: OMD Director Alarms and Remediation

Check	Remediation
load_avg_1min	Level 3: • Check the running state of the system to determine if there is an issue. If the alert is generated and resolved immediately, it may be able to be ignored. • This may or may not be an issue depending on the load/traffic on the server. If the alert continuously persists, use the `top` command from the client terminal to determine which process is running high on CPU. • Check the Grafana dashboard for any patterns in the usage.
load_avg_5min	Level 3: • Check the running state of the system to determine if there is an issue. If the alert is generated and resolved immediately, it may be able to be ignored. • This may or may not be an issue depending on the load/traffic on the server. If the alert continuously persists, use the `top` command from the client terminal to determine which process is running high on CPU. • Check the Grafana dashboard for any patterns in the usage.
load_avg_15min	Level 3: • Check the running state of the system to determine if there is an issue. If the alert is generated and resolved immediately, it may be able to be ignored. • This may or may not be an issue depending on the load/traffic on the server. If the alert continuously persists, execute the `top` command on the client terminal to determine which process is running high on CPU. • Check the Grafana dashboard for any patterns in the usage.

Check	Remediation
log_failed_notallowed	Level 3: SSH to the server as root and check the /var/log/secure file for a string similar to the following: `"User root from 11.22.33.44 not allowed because not listed in AllowUsers"`
log_failed_password	SSH to the server as root and check the /var/log/secure file for the string “Failed password”.
netstat for ESTABLISHED	SSH to the server. Check the output from the `netstat` command to determine more information about the connections and which port is being used. Look for TCP connections in the ESTABLISHED states, which could provide information about the related service.
netstat for TIME_WAIT	SSH to the server. Check the output from the `netstat` command to determine more information about the connections and which port is being used. Look for TCP connections in the TIME_WAIT states, which could provide information about the related service.
ntp_sync_status	Level 2/Level 3: Connectivity to the NTP server needs to be checked or other network resources are not responding. Use the `ntpq -p` command to check the NTP source stratum for correct time. Level 3 should fix the NTP configuration as needed, or perform additional troubleshooting to ensure that NTP is synced.
partition_usage	Level 2/Level 3: SSH to the server or view Grafana dashboards for the server to determine which partition is high on usage. After connecting to the server using SSH, look for files that are consuming a large amount of disk space.
ram_usage	SSH to the server and check the memory usage. Use commands such as `top` to identify the processes that are running and determine which processes are consuming memory. Check Grafana dashboards for any patterns in the RAM usage.

Appendix: OMD Director Alarms and Remediation

Check	Remediation
redis_status	A warning for this check indicates that an OMD Monitor node could not connect to one or more of the other OMD Monitor node. However, if OMD Monitor is installed in an HA configuration, the OMD Monitor nodes should continue to work without issue. You should investigate the reason for the loss of connection between OMD Monitor nodes. If there is no issue with connectivity, review the /var/log files on the OMD Monitor node.
service_status for grafana-server	Connect to the OMD Monitor node and enter the `systemctl status grafana-server` command to check the status of the grafana-server service. If the service is not in a running state, enter the `sudo systemctl restart grafana-server` command to try to bring it up. Note: If the grafana-server is not in a running state, the Grafana GUI will also fail to load when connected to this OMD Monitor node. Check the `/var/log/grafana/grafana.log` file for any error messages. If the alarm persists, escalate the problem for further investigation.
service_status for haproxy	Connect to the OMD Monitor node and enter the `systemctl status haproxy` command to check the status of the haproxy service. If the service is not in a running state, enter the `sudo systemctl restart haproxy` command to try to bring it up. Check the `/var/log/haproxy.log` and `/var/log/haproxy-status.log` files for any error messages. If the alarm persists, escalate the problem for further investigation.
service_status for influxdb	Connect to the OMD Monitor node and enter the `systemctl status influxdb` command to check the status of the influxdb service. Influxdb metrics may have stopped on one OMD Monitor node, however, the remaining OMD Monitor nodes will continue to store metrics. Enter the `sudo systemctl restart influxdb` command to try to bring up the influxdb service on OMD Monitor node. If the alarm persists, escalate the problem for investigation.

Check	Remediation
service_status for influxdb-relay	Connect to the OMD Monitor node and enter the systemctl status influxdb-relay command to check the status of the influxdb-relay service. Influxdb metrics may have stopped on one OMD Monitor node, however, the remaining OMD Monitor nodes will continue to store metrics. Enter the `sudo systemctl restart influxdb-relay` command to try to bring up the influxdb-relay service on the OMD Monitor node. If the alarm persists, escalate the problem for investigation.
service_status for rabbitmq-metrics-exporter	The rabbitmq-metrics-exporter service pops out metrics data from RabbitMQ and exports the same to the Monitor Nodes, InfluxDBs, and the external Kafka servers. Failure of this service would result in no metrics data in Influxdb but the Monitor mailer alerts and Uchiwa will still be functional. Connect to the Monitor node and check the status of the process using `systemctl status rabbitmq-metrics-exporter`. Inspect `/var/log/messages` on Monitor node for any error messages. Try bringing up the service using `sudo systemctl restart rabbitmq-metrics-exporter` on the Monitor node. If the alarm persists, then escalate for investigation.
service_status for rabbitmq-server	Connect to the OMD Monitor node and enter the `systemctl status rabbitmq-server` command to check the status of the rabbitmq-server service. An OMD Monitor node whose rabbitmq-server service is not running will not be monitoring any clients. Clients previously connected to this node will move to another OMD Monitor node, including the Sensu client of the OMD Monitor node whose rabbitmq-server service is not running. Inspect the `/var/log/rabbitmq/ logs` for any error messages. Enter the `sudo systemctl restart rabbitmq-server` command to try to bring up the rabbitmq-server service on the OMD Monitor node. If the alarm persists, escalate the problem for investigation.

Appendix: OMD Director Alarms and Remediation

Check	Remediation
service_status for redis	Connect to the OMD Monitor node and enter the `systemctl status redis` command to check the status of the redis service. An OMD Monitor node whose redis service is not running will not be monitoring any clients. Clients previously connected to this node will move to another OMD Monitor node, including the Sensu client of the OMD Monitor node whose redis service is not running. Inspect the `/var/log/redis/ logs` for any error messages. Enter the `sudo systemctl restart redis` command to try to bring up the redis service on the OMD Monitor node. If the alarm persists, escalate the problem for investigation.
service_status for redis-sentinel	Connect to the OMD Monitor node and enter the `systemctl status redis-sentinel` command to check the status of the redis-sentinel service. Inspect `/var/log/redis/ logs` for any error messages. Enter the `sudo systemctl restart redis-sentinel` command to try to bring up the redis-sentinel service on the OMD Monitor node. If the alarm persists, escalate the problem for investigation.
service_status for sensu-server	Connect to the OMD Monitor node and enter the `systemctl status sensu-server` command to check the status of the sensu-server service. Inspect the `/var/log/sensu/sensu-server.log` file for any error messages. Enter the `sudo systemctl restart sensu-server` command to try to bring up the sensu-server service on the OMD Monitor node. If the alarm persists, escalate the problem for investigation.
service_status for splunk	The Splunk service is down on the OMD Insights nodes. Log in to the OMD Insights nodes and enter the command `systemctl status splunk` to check the status of the Splunk service. The status of the service should show “running”.

Check	Remediation
service_status for tcp-rabbitmq-exchange	The tcp-rabbitmq-exchange service collects Sensu checks output from the TCP handler and sends the metrics data to the RabbitMQ on the same Monitor node. Failure of this service would result in no metrics data in Influxdb, but Monitor mailer alerts and Uchiwa will still be functional. Connect to the Monitor node and check the status of the process using the command `systemctl status tcp-rabbitmq-exchange`. Inspect `/var/log/messages` on the Monitor node for any error messages. Try bringing up the service using `sudo systemctl restart tcp-rabbitmq-exchange` on the Monitor node. If the alarm persists, then escalate for investigation.
sshd_running_status	Log in to the server through the console and check whether the sshd service is running. If it is not running, start the sshd service and escalate to Level 3.
swap_usage	Try to determine which processes are consuming the swap memory on the system raising the alarm. This issue needs to be escalated ASAP.
tcp_connection	Level 3 should look at the running state of the system to determine if there are any issues. Use the `netstat` command to check how the connections are distributed.
tripwire_running_status	Level 3 should address all issues with these alarms. Level 2 should take no action unless Level 3 determines there is an issue. To clear an alarm, connect to the server and switch to root. Look at the history for the tripwire command. Run the command to set files and then run the command `/usr/sbin/tripwire --check` to ensure there are no violations.

Appendix: OMD Director Alarms and Remediation