Cisco Virtual Media Packager User Guide

Software Version 2.8.2

First Published: March 2017

Cisco Virtual Media Packager User Guide

Preface

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

- Audience, page 3
- Document Organization, page 3
- Document Conventions, page 3
- Related Publications, page 4
- Obtaining Documentation and Submitting a Service Request, page 4

Audience

This guide is for the networking professional managing the Virtual Media Packager (VMP) software product. Before using this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of Ethernet, local area networking, and Internet streaming.

Document Organization

This guide includes the following chapters:

Chapter or Appendix	Description
VMP Overview, page 5	Describes the VMP and its components, features, and prerequisites.
Deploying the VMP, page 25	Describes how to deploy the VMP components.
VMP Service Manager GUI Reference, page 71	Describes how to use the VMP Manager graphical user interface (VMP-M GUI) to configure the VMP.
Troubleshooting VMP Problems, page 121	Provides information and procedures for troubleshooting VMP problems.

Document Conventions

This guide uses basic conventions to represent text and table information.

Convention	Description
boldface font	Commands, keywords, and button names are in **boldface**.
italic font	Variables for which you supply values are in *italics*. Directory names and filenames are also in italics.
`screen` font	Terminal sessions and information the system displays are printed in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Variables you enter are printed in *`italic screen`* font.
string	Defined as a nonquoted set of characters. For example, when setting a community string for SNMP to “public,” do not use quotation marks around the string, or the string will include the quotation marks.
vertical bars (|)	Vertical bars separate alternative, mutually exclusive, elements.
< >	Variable for which you supply a value.
{ }	Elements in braces are required elements.
[ ]	Elements in square brackets are optional.
{**x** | **y** | **z**}	Required keywords are grouped in braces and separated by vertical bars.
[**x** | **y** | **z**]	Optional keywords are grouped in brackets and separated by vertical bars.
[{ }]	Braces within square brackets indicate a required choice within an optional element.

Note: Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in the manual.

Note: Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Related Publications

Refer to the following documents for additional information about *VMP*:

- *Release Notes for Virtual Media Packager 2.8*
- Cisco *Virtual Media Packager 2.8* API Guide
- *Open Source Used in Virtual Media Packager 2.8*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

VMP Overview

This chapter provides the following information:

- Product Description, page 5
- nInsys–Widevine DASH Encryption., page 5
- Features, page 11
- System Requirements, page 21
- Restrictions and Limitations, page 23

What's NEW

This release of VMP incorporates feature enhancements and introduces support for:

- Insys–Widevine DASH Encryption.

Product Description

Media origination is a critical function for the delivery of advanced revenue-generating media services to consumers. The Virtual Media Packager (VMP) provides critical functions required to capture, store and originate media for multi-screen consumption. The VMP primarily provides the enabling functions in the media data plane. The VMP works with other external components, such as encoders, transcoders, control applications, and end-client applications, to form the end-to-end media service ecosystem.

The VMP incorporates the following elements:

- Networks, page 5
- Platform and Applications Manager (PAM), page 9 and VG
- Media Capture Engine Worker (MCE-Worker), page 10
- Centralized Logging System (CLS), page 11
- AppEngine, page 11

Networks

The VMP networks connect the VMP components to each other, and with external appliances and services.

- Management–Primary VMP network that connects all of the components.

  AppEngine - A minimum of 6 app engines (2 Redis, 2 HAProxy, and 2 IPVS) are required to enable Media Service.

- Data In–Ingest network. It connects the MCE-Workers and MPE-Workers.

For MCE-Workers, the Data In network serves as the Live or VOD ingest interface and can be shared with other components.

For MPE-Workers, the Data In interface corresponds to the input from the MCE-Workers' Data Out interface, and it is shared only with other MCE-Workers and MPE-Workers.

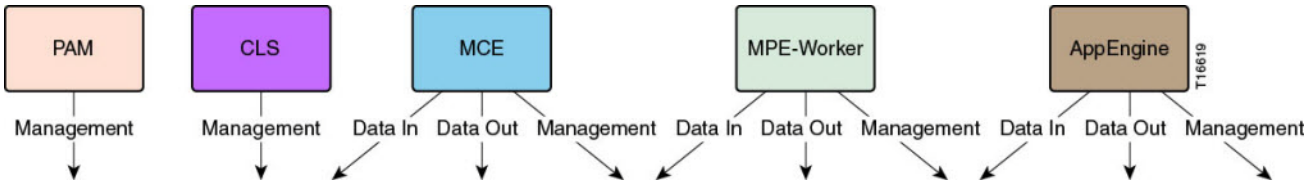
- Data Out—Streaming network. It connects the MCE-Workers and MPE-Workers.

  For the MPE-Workers, the Data Out network provides the external Apple HTTP Live Streaming (HLS) or Microsoft HTTP Smooth Streaming (HSS) or Dynamic Adaptive Streaming over HTTP (DASH-MP4) stream feeds to clients.

The following table shows the component-to-network mapping.

Component	Network Connections
PAM	Management
CLS	Management
MCE-Worker	Management, Data In, Data Out
AppEngine	Management, Data In, Data Out
MPE Worker	Management, Data In, Data Out

Figure 1 VMP Device-to-Network Mapping

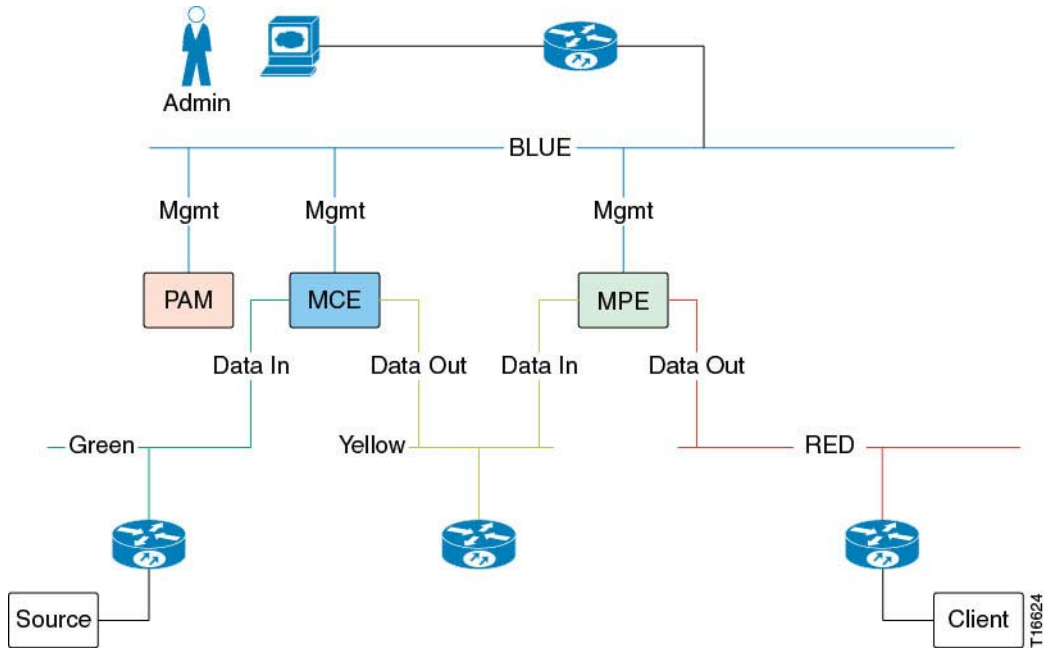


Based on the device-to-network mapping, the administrator can choose to combine or separate the networks in different ways. For example, you might want to keep multicast Live streams separate, or keep unencrypted content separate from the ingest network or the MCE output streams.

The following network topologies are some of the possible configurations.

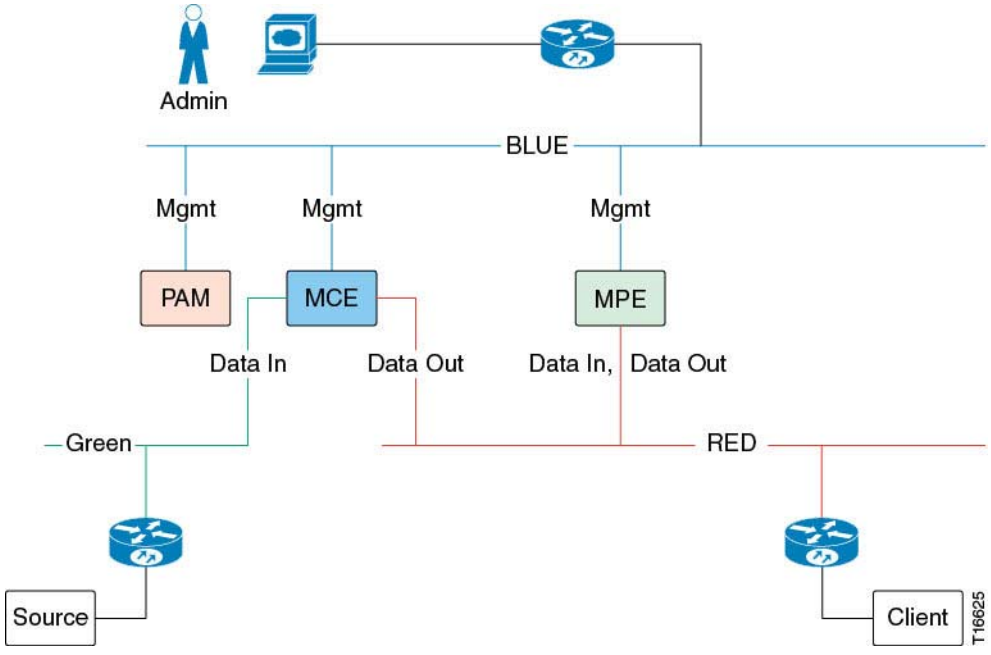
- Four separate and distinct networks, here labeled Blue, Green, Yellow, and Red. The devices are interconnected by switches or routers.

Figure 2 Four Networks



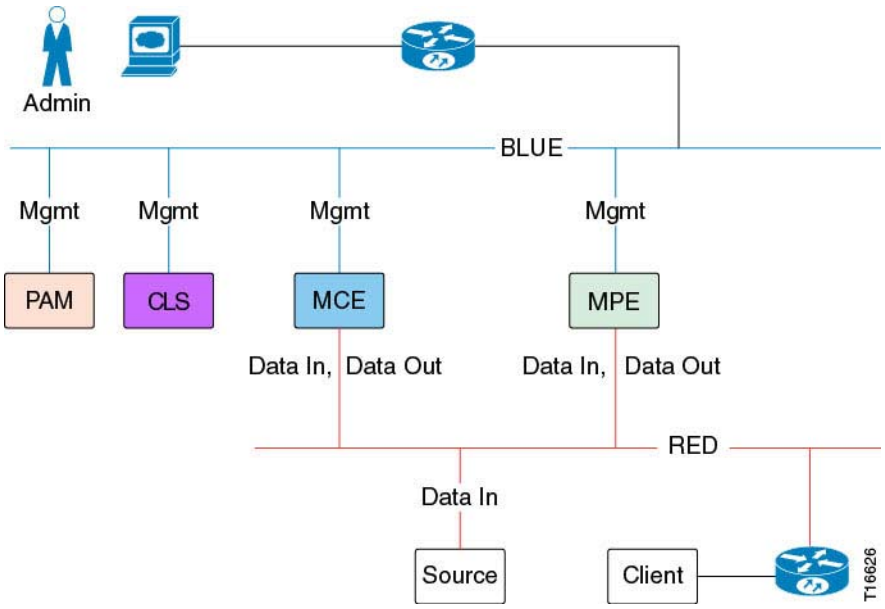
- Three separate and distinct networks, one for Management (Blue), one for Data In (Green), and one for Data Out (Red). The devices are interconnected by switches or routers.

Figure 3 Three Networks



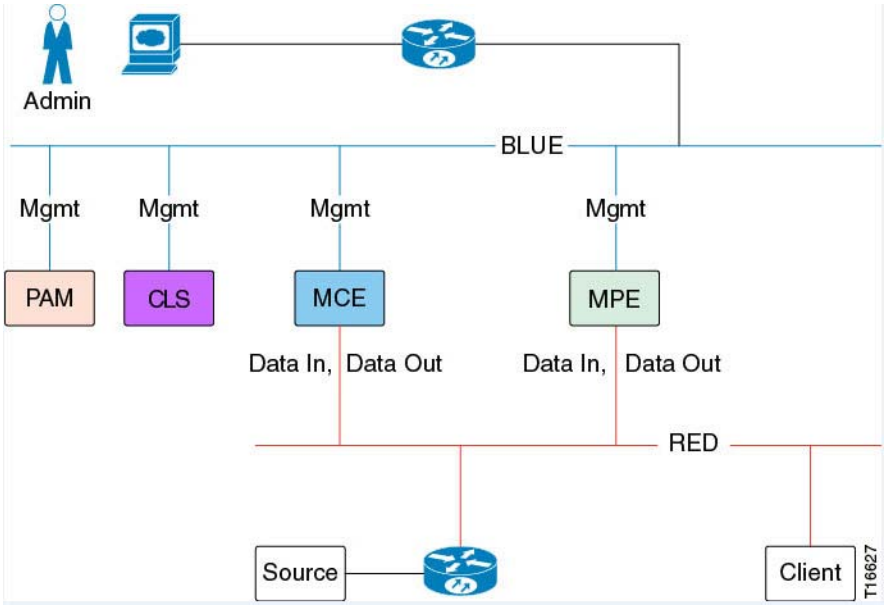
- Two separate and distinct networks, one for Management (Blue), one for Data In and Data Out (Red). The devices, including the client, are interconnected by switches or routers.

Figure 4 Two Networks: Management and Data In/Out, Client Connected via Switch or Router



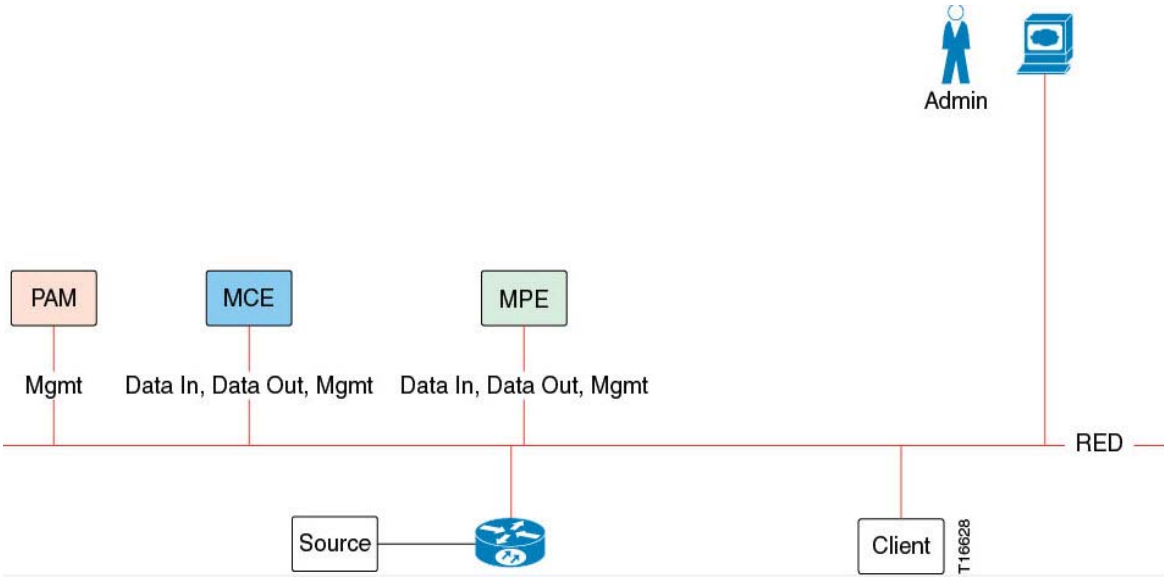
- Two separate and distinct networks, one for Management (Blue), one for Data In and Data Out (Red). The devices, including the source, are interconnected by switches or routers.

Figure 5 Two Networks: Management and Data In/Out, Source Connected via Switch or Router



- One combined network. The devices are all connected to the same switch or router.

Figure 6 One Network



Platform and Applications Manager (PAM)

The VMP uses the PAM to install, configure, monitor, and recover the other VMP components. The PAM also orchestrates load-balancing and security functions, ensures secure connectivity, and provides low-level network services such as DNS and NTP.

VMP requires three (3) PAMs.

Note: If you need to release a PAM VM for any reason, do not power it off from the VMware console. Instead, to maintain failover of ongoing Live and VOD tasks, you must shut down and restart the PAM VM.

The PAM VM contains the following applications.

Platform Manager

The Platform Manager maintains the details of all of the VMP virtual machines (VMs) and reports the VMs and other configured appliances to the Service Manager.

The Platform Manager also hosts the following elements:

- The Domain Name System (DNS) server
- The Network Time Protocol (NTP) server

Service Manager

The Service Manager provides the following services for the VMP:

- Applies the appropriate configuration to the MPE.
- Monitors the entire VMP.
- Initializes and starts the HTTPS user interface into the VMP.
- Uses node information provided by the Platform Manager, as well as its own default settings, to discover and configure the available nodes.

- Provides a set of REST APIs to create and manage Live-to-VOD & CDVR service instances.
- Reports the status of managed nodes to users when queried.

Document Server (DocServer)

The DocServer provides a persistent data store for VMP configuration and monitoring data (other than error and transaction logs).

MongoDB Database

MongoDB provides a persistent store for configuration and other operational data.

Redis

Redis provides an in-memory non-persistent store for runtime data.

Apache ZooKeeper

The Apache ZooKeeper provides coordination and light state maintenance and notification for the VMP.

Service Instance Controller (SIC)

The SIC obtains service-specific input from the configuration and creates the application instances required for the service.

Application Instance Controller (AIC)

The AIC installs all of the components required for an MCE or MPE application instance.

Media Capture Engine Task Controller (MCE-TC)

The MCE-TC allocates and load-balances capture tasks among the MCE-Workers. The MCE-TC also manages the lifecycle (start, stop, update, and monitor) of each capture task and session; provides resiliency and redundancy for the tasks; and tracks, handles, and reports any task failures.

Asset Workflow Manager (AWM)

The AWM configures asset workflows that span multiple applications.

Key Management Server (KMS) Proxy

The KMS proxy acts as a proxy to external KMS systems, such as Key Store, Verimatrix, and Irdeto. The KMS proxy helps synchronize keys among multiple MPE-Workers, avoiding redundant calls to external systems, and provides the support functions required for internal content protection, such as key generation and key rotation.

Media Capture Engine Worker (MCE-Worker)

The MCE-Workers performs the capture tasks for Live-to-VOD. The MCE-Workers acquire, prepare, index, and store media content from various sources. The MCE-Worker also converts those contents to Common Intermediate Format (CIF) assets that can then be transformed into different end-client formats by the Media Playback Engine (MPE).

The following table lists the inputs, storage formats, and output formats supported by the MCE for services.

Service	Function	Input	Storage Formats	Output Formats (From the MCE)
Live	Linear Stream Acquisition–Time-Shift Recording	ATS (UDP Multicast, UDP Unicast)	ATS with CIF,	CIF
VOD	VOD Acquisition	CIF ATS VOD	CIF ATS VOD	CIF
Live-to VOD	Live-to-VOD	ATS (UDP Multicast	CIF ATS VOD with CIF Indexing	CIF ATS VOD with CIF Indexing

Media Playback Engine Worker (MPE-Worker)

The MPE-Worker is the VMP just-in-time packager (JITP), used for Live and VOD video playout. The MPE processes incoming requests for manifests, segments, fragments, and other related resources, and plays recorded content to multi-screen IP-connected ABR endpoints, such as smart phones, tablets, smart TVs and set-top boxes (STBs) with ABR playout capability.

Centralized Logging System (CLS)

The CLS provides a central location for the aggregation, analysis, and display of VMP error logs and events.

AppEngine

A minimum of 6 app engines (2 Redis, 2 HAProxy, and 2 IPVS) are required to enable Media Service.

Features

- Overview, page 11
- VMP Service Manager GUI, page 13
- High Availability (HA), page 13
- Features Supported for Live/VOD Streaming, page 15
- Features Supported for VOD Only, page 20

Overview

Feature Set	Features
Components	The following VMP software components are required for a MPE setup: ■ Platform and Applications Manager (PAM) VMP requires three (3) PAMs. ■ Media Playback Engine (MPE) ■ Media Capture Engine Worker (MCE-Worker) ■ AppEngines (6) ■ CLS
VMware Virtualization	■ Deployment of the VMP as a set of virtual machines (VMs) via an Open Virtual Appliance (OVA) image
Management	■ Configuration of platform services (DNS, NTP) ■ Mapping of virtual networks (Management, Data In, Data Out) ■ Configuration of the VMP system ■ System health monitoring ■ Unified management for COS

Feature Set	Features
Application Programming Interfaces	■ Provisioning of resources, such as channels ■ Provisioning of recording services and policies ■ Provisioning of recordings ■ Providing recorded asset information ■ Provisioning of playout services ■ Provisioning of content protection ■ Provisioning of HTTP media sources ■ Monitoring VMP health ■ Displaying system diagnostics ■ Displaying service diagnostics ■ Displaying logs ■ Displaying events
Service Routing	■ DNS service routing ■ Load-based routing ■ Application failure detection
Ingest and Recording	■ Ingest and recording of content with the following formats: – Adaptive transport stream (ATS) ■ Ingest and recording of content with the following codecs: – H.264 (AVC) – H.265 (HEVC) Note: H.264 supports HLS and HSS publish. H.265 only supports HLS publish.
On-Demand Encapsulation (ODE) of Adaptive Bitrate (ABR) Content for Live and VOD Origination with CIF Indexing	■ ODE Playout for HLS, HSS and DASH-MP4 formats ■ Trick-mode support for ODE-HLS and ODE-HSS ■ PlayReady DRM and AES-128-CTR encryption for ODE-HSS
Key Management Server (KMS) Support for ODE	■ Advanced Encryption Standard (AES)—Standard HLS only ■ Key acquisition from Adobe License Server—Adobe Access HLS, VG DRM and Insys DRM ■ Key acquisition from Cisco Key Store 1.1—Standard HLS only ■ Key acquisition support with Irdeto—Standard HLS and PlayReady HSS ■ Key acquisition support with Verimatrix Video Content Authority System (VCAS) 3.3—Standard HLS and PlayReady HSS ■ Key acquisition support for DASH

Feature Set	Features
Cache-Control	■ Cache-control header support for VOD service origination (HLS, HSS and DASH-MP4) ■ If-Modified-Since (IMS) support for VOD and Live services (HLS, HSS and DASH)-MP4
High Availability (HA)	■ Redundancy of PAM VMs ■ Basic load-balancing of MCE-Workers and MPE-Workers ■ Redundancy for Asset Capture Sessions for Live and Live-to-VOD
VMP Service Manager GUI	■ Configuration of Live, VOD, and Live-to-VOD workflows within the same service instance
Logging, Status Reporting, and Troubleshooting	■ Monitoring, system and service diagnostics, and display of logs and events in the VMP Service Manager GUI ■ Error and transaction logs ■ Node status ■ Detailed troubleshooting procedures

VMP Service Manager GUI

The VMP Manager GUI (VMP Service Manager GUI) enables you to quickly and easily configure the VMP infrastructure, service domain objects, and Live and VOD services. The GUI also provides valuable monitoring functions, including AWM statistics, system diagnostics, service diagnostics, log display and analysis, and event display.

For more information about the GUI, including how to launch it, see Working with the VMP Service Manager GUI, page 73.

For more information about enabling logging, see the Setting Up the CLS, page 33.

High Availability (HA)

The PAM has two classes of components for HA:

- Third party components, such as ZooKeeper, MongoDB, and Redis, use their own proprietary clustering and redundancy schemes.
- Cisco components, such as the VMP Service Manager GUI and DocServer, use ZooKeeper for leader selection.

In an HA environment, multiple PAM VMs provide redundancy for the applications that run on the PAM.

HA requires at least three PAM VMs, because applications such as ZooKeeper, MongoDB, and Redis require at least three components to form a working cluster.

Many of these applications also require a majority in order to form a quorum. That is, a cluster of three components can recover from the failure of a single component, because there are still two components to form a majority. But if two components fail, the single remaining component is not a majority, and the cluster cannot recover until one of the failed components recovers.

Therefore, we must configure three PAM VMs, to ensure recovery in the event of multiple failures, and to support high performance, especially the sharing of databases and other applications.

Note: If you need to release a PAM VM for any reason, do not power it off from the VMware console. Instead, to maintain failover of ongoing Live and VOD tasks, you must shut down and restart the PAM VM.

For information about deploying PAM VMs for HA, see the Configuring the VMP Using the VMP Manager GUI, page 50.

Monitoring with the VMP Service Manager GUI

The VMP Service Manager GUI provides valuable monitoring functions, including system diagnostics, service diagnostics, logging, and events. For more information, see the following sections:

- Displaying High-Level Overview Information for the VMP, page 76
- Displaying System Diagnostics, page 112
- Displaying Service Diagnostics, page 114
- Analyzing Logs, page 117
- Analyzing Logs, page 117
- Displaying Events, page 118

Closed Captioning/Subtitles

The VMP supports:

- All data related to Closed Captions or subtitles in the input source is preserved.
- MCE creates Timed Text Markup Language (TTML) data as a storage format by parsing the closed caption data from the input source.
- For US markets, Closed Captions format CEA-608 is supported.
- For Europe, teletext ETS 300 706 is supported, our current implementation is at presentation level 1.5.
- The client (player) reads TTML data through MPE, outputting each line of text on the screen in accordance with the 'begin' and 'end' time.
- No steps are required to enable TTML generation; this data will be generated if captions are present in the input stream.

Event Signaling and Management (ESAM)

The VMP supports CableLabs ESAM for real-time dynamic ad insertion for VOD HLS. There are two methods for Ad insertion- 1. ESAM POIS Callout and 2. ESAM Template. Currently, SCTE 35 time signal_ command is supported.

ESAM Template

The MCE uses the ESAM Template format to embed scte35 tag information in the Media Presentation Description (MPD) file, along with the segment's presentation timestamp (PTS) and the duration of the event. The MPE then obtains the MPD file and generates an HLS or HSS client manifest with the corresponding tags inserted. The template is then provisioned on the system by the service provider based on the ADS vendor.

ESAM Placement Opportunity Information System (POIS) Callout

The VMP processes real-time signals, such as SCTE 35, and generates real-time manifests. A real-time transcoder submits an SCTE 35 time_signal command message to a Placement Opportunity Information System (POIS). The POIS confirms the validity of the signal and returns information that enables the transcoder to identify and update the start and end times of a signal region. The returned information can also include signal region durations, which can be used for conditioning the stream that is being encoded, and auxiliary data to be inserted into the video stream for use by downstream systems.

The MCE communicates with the POIS server through an internal ESAM proxy using HTTP POST requests. The POIS responds with tag information which the MCE embeds in the Media Presentation Description (MPD) file, along with the segment's presentation timestamp (PTS) and the duration of the event. The MPE then obtains the MPD file and generates an HLS client manifest with the corresponding tags inserted.

For information about configuring ESAM profiles, see the Configuring ESAM Profiles, page 100.

Support for Envivio Encoders

For ABR publishing, the VMP requires adaptive transport stream (ATS) input data that complies with the CableLabs OpenCable OC-SP-ATS-I01-140214 and OC-SP-EBP-I01-130118 specifications. The minimum requirement for input data is an ATS with video fragment Encoder Boundary Point (EBP) markers, synced across all ABR profiles.

The VMP supports the Envivio encoder, which fulfills this requirement; the VMP provides any missing audio EBP and video segment EBP markers. Transcoders like CMP and DCM provide additional information in the input ATS data, such as audio EBP, video segment EBP, and video fragment EBP markers.

There is no configuration required to enable this support.

Support for MPE-Worker IP Address with FQDN

The VMP supports IP addresses with FQDNs for MPE-Workers.

For example, the following URL format is supported for HLS client requests:

```
http://AssetWorkFlow-name.FQDN/AssetWorkFlow-name/Content-ID/Content-ID.m3u8
http:///AssetWorkFlow-name/Content-ID/Content-ID.m3u8
```

The following URL format is supported for HSS client requests:

```
http://AssetWorkFlow-name.FQDN/AssetWorkFlow-name/Content-ID/Content-ID.ism/Manifest
http://DATAOUT_IPAddressOfMPE/AssetWorkFlow-name/Content-ID/Content-ID.ism/Manifest
```

The following URL format is supported for DASH

```
http://dash.edgesuite.net/akamai/bbb_30fps/bbb_30fps.mpd
http://dash.edgesuite.net/akamai/test/caption_test/ElephantsDream/elephants_dream_480p_heaac5_1.mpd
```

There is no configuration required to enable this support.

Support for HLS PID Passthrough

The VMP supports HLS PID passthrough. The published HLS version 3 URL supports this feature. To enable it, you must add a HLS version 3 variant playlist for a publish template that will be used. For more information, refer to Configuring Publish Templates, page 108.

Support for DVB Bitmap Subtitles

The VMP supports transforming or passthrough of DVB bitmap subtitles from ATS to HLS. When Transform mode is configured, VMP converts the DVB bitmap subtitle to SMPTE-TT formatted subtitle, encapsulates them into ID 3 tags and muxes them with .ts files of HLS. When Passthrough mode is configured, VMP preserves the DVB bitmap subtitles in ATS and keeps them intact in the .ts files of HLS.

Features Supported for Live/VOD Streaming

The VMP supports the following features for Live/VOD streaming:

- ATS Input with EBP for HLS, HSS and DASH-MP4, page 16

- Advanced Audio Coding Low-Complexity (AAC-LC) for HLS, HSS and DASH-MP4, page 16
- Key Rotation for HLS, page 16
- Key Acquisition for HLS, HSS and DASH-MP4, page 16
- Multi-Language Audio for HLS, HSS and DASH-MP4, page 17
- Trick Mode for HLS and HSS, page 17
- Variant Playlists for HLS, HSS and DASH-MP4, page 17
- DVR Window for HLS, HSS and DASH-MP4, page 20
- Support for Content ID Mapping for Irdeto for HLS and HSS, page 20
- Support HLSv7: EXT-X-Start, page 20

ATS Input with EBP for HLS, HSS and DASH-MP4

The process of capturing, transferring, or otherwise importing Live content is known as Live ingest. The VMP supports the ingest and storage of Live content delivered by adaptive bitrate (ABR) streaming over HTTP, and the delivery of the content to the end clients. The VMP ingests Live content in ATR format with EBP. The formats required by the end clients, such as HLS, HSS and DASH-MP4, are produced on-demand by the MPE-Workers.

The VMP uses the Alliance for Telecommunication Industry Solutions () index format specification for MPEG-2 TS media files.

There is no configuration required to enable this support.

Advanced Audio Coding Low-Complexity (AAC-LC) for HLS, HSS and DASH-MP4

The VMP supports AAC-LC audio compression for HLS, HSS and DASH-MP4 Live capture of MPEG-2 TS media files.

There is no configuration required to enable this support.

Key Rotation for HLS

The VMP supports internal key generation with key rotation for Live HLS playout. The VMP provides KMS proxy and key generation as a single task for each Live service. The VMP maintains an internal cache of key encryption information for each Live stream and for each rotation point within each stream. Key generation is triggered on the first client request for a Live playout and at each subsequent rotation point in the playout. The VMP generates the encryption keys algorithmically using a key seed and then caches the keys. The presentation time stamp (PTS) values are used as an index to mark rotation points.

For information about configuring variant playlists, see the Configuring Publish Templates, page 108.

Key Acquisition for HLS, HSS and DASH-MP4

The VMP supports the following KMS types:

- Adobe License Server—Adobe Access HLS, Insys, VGC, & DRM
- Advanced Encryption Standard (AES)—Standard HLS only
- Cisco Key Store 1.1—Standard HLS, VG DRM, & Insys DRM
- Irdeto PlayReady—Standard HLS and PlayReady HSS only
- Verimatrix Video Content Authority System (VCAS) 3.3—Standard HLS and PlayReady HSS

- EZDRM—Common DASH encryption
- BUYDRM—Common DASH encryption
- Insys—Widevine DASH Encryption

For information about enabling key acquisition, see the Configuring Key Profiles, page 101.

Multi-Language Audio for HLS, HSS and DASH-MP4

The VMP supports multi-language audio for Live HLS, HSS and DASH-MP4 playout.

There is no configuration required to enable this support.

Trick Mode for HLS and HSS

Trick mode, also known as trick play, provides functions such as fast-forward and rewind for digital video systems. The VMP supports trick mode with I-frame playlists for HLS, HSS Live playout and VOD.

There is no configuration required to enable this support.

Variant Playlists for HLS, HSS and DASH-MP4

Variant playlist support enables you to select the video streams to include in a manifest by configuring a list of video and audio bitrates in the VMP Service Manager GUI. The VMP supports video bitrate selection (HLS, HSS and DASH-MP4) and audio bitrate selection (HSS and DASH-MP4).

For more information about configuring variant playlists, see the Configuring Publish Templates, page 108.

Sample HLS Playlist (.m3u8)

```
#EXTM3U
#EXT-X-TARGETDURATION:10
#EXT-X-VERSION:4
#EXT-X-MEDIA-SEQUENCE:1
#EXT-X-PLAYLIST-TYPE:EVENT
#EXTINF:10
12345/0.ts
#EXTINF:10
12345/900000.ts
#EXT-X-DISCONTINUITY
#EXT-X-SIGNAL-START:SignalID=Start Ad 1
#EXTINF:10
12345/1800000.ts
#EXT-X-SIGNAL-SPAN:SignalID=Start Ad 1,TimeFromSignalStart=10
#EXTINF:10
12345/2700000.ts
#EXT-X-SIGNAL-END:SignalID=End of avail
#EXT-X-DISCONTINUITY
#EXTINF:10
12345/3600000.ts
#EXTINF:10
12345/4500000.ts
#EXTINF:10
12345/5400000.ts
#EXTINF:10
12345/6300000.ts
#EXTINF:10
12345/7200000.ts
#EXTINF:10
12345/8100000.ts
```

```
#EXTINF:10
12345/9000000.ts
```

Sample HSS Playlist (.ismc)

```
<StreamIndex Type=”text” Name=”scte35” SubType=”SCTE35” Chunks=”0” Timescale=”10000000”
Url=”QualityLevels({bitrate})/Fragments(scte35
<QualityLevel Index=”0” Bitrate=”100” CodecPrivateData=”” FourCC=”text”/>
<c t=”200000000” d=”100000000”>
<f>
PEFjcXVpcmVkU2lnbmFsCiAgICAgICAgICAgIHhtbG5zOmNvcmU9Imh0dHA6Ly93d3cuY2FibGVsYWJzLmNvbS9uYW1lc3BhY2VzL21
ldGFkYXRhL3hzZC9jb3JlLzIiCgkgIC
</f>
</c>
<c t=”400000000” d=”100000000”>
<f>
PEFjcXVpcmVkU2lnbmFsCiAgICAgICAgICAgIHhtbG5zOmNvcmU9Imh0dHA6Ly93d3cuY2FibGVsYWJzLmNvbS9uYW1lc3BhY2VzL21
ldGFkYXRhL3hzZC9jb3JlLzIiCgkgIC
</f>
</c>
</StreamIndex>
```

Sample DASH-MP4 manifest file(.ismc)

```
<?xml version="1.0" encoding="UTF-8"?>
 <MPD
         mediaPresentationDuration="PT8072S"
         minBufferTime="PT4S"
         profiles="urn:mpeg:dash:profile:isoff-on-demand:2011"
         type="static"
         xmlns="urn:mpeg:dash:schema:mpd:2011"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="urn:mpeg:dash:schema:mpd:2011
http://standards.iso.org/ittf/PubliclyAvailableStandards/MPEG-DASH_schema_files/DASH-MPD.xsd">
         <Period
                 id="1"
                 start="PT0S">
                 <AdaptationSet
                         bitstreamSwitching="false"
                         lang="pol"
                         mimeType="audio/mp4"
                         segmentAlignment="false"
                         startWithSAP="1">
                         <SegmentTemplate
                                 initialization="$RepresentationID$/init.mp4"
                                 media="$RepresentationID$/$Time$.m4f"
                                 startNumber="0"
                                 timescale="90000">
                                 <SegmentTimeline>
                                         <S
                                                 d="180480"
                                                 r="5"
                                                 t="0"/>
                                         <S
                                                 d="188160"
                                                 r="0"
                                                 t="1082880"/>
                                         <S
                                                 d="170880"
                                                 r="0"
                                                 t="1271040"/>
                                         <S
                                                 d="180480"
                                                 r="2"
                                                 t="1441920"/>
```

```
                        </SegmentTimeline>
                    </SegmentTemplate>
                    <Representation
                        audioSamplingRate="48000"
                        bandwidth="53625"
                        codecs="mp4a.40.2"
                        id="53625_audio_frag_80_53625_2023"
                        numChannels="2"/>
                    <Representation
                        audioSamplingRate="48000"
                        bandwidth="114375"
                        codecs="mp4a.40.2"
                        id="114375_audio_frag_80_114375_2023"
                        numChannels="2"/>
                </AdaptationSet>
                <AdaptationSet
                    bitstreamSwitching="false"
                    mimeType="video/mp4"
                    segmentAlignment="true"
                    startWithSAP="1">
                    <SegmentTemplate
                        initialization="$RepresentationID$/init.mp4"
                        media="$RepresentationID$/$Time$.m4f"
                        startNumber="0"
                        timescale="90000">
                        <SegmentTimeline>
                            <S
                                d="180180"
                                r="4032"
                                t="0"/>
                        </SegmentTimeline>
                    </SegmentTemplate>
                    <Representation
                        bandwidth="700000"
                        codecs="avc1.42C00C"
                        height="192"
                        id="video_frag_auto_700000_20233"
                        width="320"/>
                    <Representation
                        bandwidth="1300000"
                        codecs="avc1.42C01F"
                        height="464"
                        id="video_frag_auto_1300000_20234"
                        width="800"/>
                    <Representation
                        bandwidth="1800000"
                        codecs="avc1.42C01F"
                        height="576"
                        id="video_frag_auto_1800000_20235"
                        width="1024"/>
                    <Representation
                        bandwidth="3600000"
                        codecs="avc1.64001F"
                        height="720"
                        id="video_frag_auto_3600000_20237"
                        width="1280"/>
                </AdaptationSet>
        </Period>
</MPD>
```

DVR Window for HLS, HSS and DASH-MP4

The VMP supports a DVR window feature, also called a time-shift buffer, for Live HLS, HSS and DASH-MP4 capture.

The DVR window, also called the time-shift buffer, is the length of time, in seconds, that Live content is stored with respect to the current Live point. The DVR window enables an end client to rewind to a previous point in a Live capture, as long as it does not exceed the configured duration of the DVR window (or the beginning of the capture). As the current Live point moves, content older than the DVR window is deleted, maintaining a constant DVR window for the Live service.

For a Live service, the MCE captures the Live multicast or unicast feed, indexes it, and stores the metadata, transport stream files, and TTML files. The VMP provides support for two types of storage- COS and NAS and both can be used for TSTV/DVR window usage.

For information about configuring the DVR window, see the Configuring Asset Lifecycle Policies, page 104.

Support for Content ID Mapping for Irdeto for HLS and HSS

The Irdeto Control API requires unique content IDs for HLS and HSS key acquisition.

For example, given content ID **CiscoTest1**, the HLS key must be retrieved from Irdeto Control with **CiscoHLSTest1**, and the HSS key with **CiscoHSSTest1**. This results in over-provisioning of content in the VMP: one Live or VOD asset for HLS, and another for HSS. Content ID mapping for Irdeto avoids this over-provisioning.

To enable content ID mapping for Irdeto for a Live service, add one or more sets of acquisition details to the Acquisition table for a channel in a channel lineup. For more information, see the description of the Acquisition table in the Configuring Channel Lineups, page 95.

Support HLSv7: EXT-X-Start

This feature allows the user to specify a start time (VOD)/delay time (LIVE) for the player within the Live or VOD asset. The time is indicated by the “#EXT-X-START” tag in the stream manifests.

VOD Application:

If the user wants to start play from an arbitrary point in an asset, multiple urls (variants) can be created for various playback times from a single ingested asset.

LIVE Application:

If the user wants to delay time in live playback sessions. Delays are often used on live streaming sites such as twitch.tv. and is required for live online gaming tournaments to prevent spectators from relaying stream information to competitors.

Features Supported for VOD Only

For information about Live services, see the Creating Unified Media Services, page 50.

Ingest and Storage of the ATS Package for HLS, HSS and DASH-MP4

Video-on-demand (VOD) enables service providers to syndicate contents from various content providers and distribute the contents to their subscribers. The process of capturing, transferring, or otherwise importing VOD content is known as VOD ingest.

The VMP supports the ingest and storage of VOD content delivered by ABR streaming over HTTP, and the delivery of the content to the end clients. The VMP ingests VOD content in ATS format and stores it in a NAS store. The formats required by the end clients, such as HLS, HSS and DASH MP4, are produced on-demand by the MPE-Workers.

The VMP uses the and DASH index formats and the specification for MPEG-2 TS media files.

Performance Enhancements

The VMP supports the ingest of up to 20 VOD packages at the same time.

There is no configuration required to enable this support.

System Requirements

External Servers

Configuring external DNS, NTP servers is mandatory for all VMP components (MCE, AppEngines, CLS and MPE.

Cisco UCS

All of the VMP components run on top of VMware on Cisco Unified Computing System (UCS) B200 M3 Blade Servers. For information about running the VMP components on other types of servers, contact your Cisco representative.

The following table shows the minimum UCS hardware requirements for the VMP:

Table 0-1

Part Number	Description	Quantity
UCSB-B200-M3-U	UCS B200 M3 Blade Server w/o CPU, mem, HDD, mLOM/mezz (UPG)	4
UCS-CPU-E52680B	2.80 GHz E5-2680 v2/115W 10C/25MB Cache/DDR3 1866MHz	2 (Total 40 CPUs)
UCS-MR-1X082RY-A	8GB DDR3-1600-MHz RDIMM/PC3-12800/ dual rank/1.35v	16 (Total 128 GB)
A03-D600GA2	600GB 6Gb SAS 10K RPM SFF HDD/hot plug/ drive sled mounted	2 (1200 GB total disk space available)
UCSB-MLOM-40G-01	VIC 1240 modular LOM for M3 blade servers	2
UCSB-HS-01-EP	Heat Sink for UCS B200 M3 server	2

VMware, vCenter, vSphere

VMP support for VMs requires the following virtualization software programs and releases:

- VMware ESXi hypervisor version 5.1 or later, running on the server
- VMware vCenter version 5.1 or later
- VMware vSphere version 5.1 or later

The following table shows the minimum DL380 hardware requirements for the VMP:

Table 0-2

Part Number	Description	Quantity
653200-B21	HP DL380p Gen8 8-SFF CTO Chassis	1
715224-L21 ■ HA839A1 ■ HA867A1	HP DL380p Gen8 E5-2697v2 FIO Kit HP Factory Express Server System Custom SVC HP Data Express Standard Server SVC	1 1 1
715224-B21	HP DL380p Gen8 E5-2697v2 Kit	1
708641-B21	HP 16GB 2Rx4 PC3-14900R-13 Kit	16
652605-B21	HP 146GB 6G SAS 15K 2.5in SC ENT HDD	2
665249-B21	HP HP560SFP+ 10GbE 2P Server Adapter	1
661069-B21	HP 512MB FBWC for P-Series Smart Array	1
656363-B21	HP 750W CS Platinum Plus Hot Plug Power Supply Kit	2
684208-B21	HP 1GbE 4-port 331FLR Adapter FIO Kit	1
AF556A	PWR CRD KT 1.83m 10A C13-NA/JPN	2
512485-B21	HP iLO Advanced including 1yr TS U E-LTU	1
U4545E	HP 3y 4h 24x7 ProLiant DL38x HW Support	1
663478-B21	HP 2U SFF BB Rail Kit Gen8	1

VM Sizing

When deploying VMs from the SuperOVA, the following hardware resources will be allocated based on the VM type selected.

VMP Component	CPUs	RAM	Hard Drive	Hard Drive 2	Network Interfaces
PAM	4	16 GB	32 GB	NA	2 X 10 GE
MCE	8	32 GB	32 GB	NA	3 X 10 GE
MPE	8	32 GB	32 GB	NA	3 X 10 GE
AppEngines (AE)	8	32 GB	32 GB	NA	3 X 10 GE)
CLS - Small VM (< 10 VMP VMs	8	32 GB	32 GB	128GB	2 X 10 GE
CLS - Medium VM (< 100 VMP VMs	8	32 GB	32GB	256GB	2 X 10 GE
CLS - Large VM (< 200 VMP VMs)	12	48GB	32 GB	512GB	2 X 10 GE

These recommended minimum system resource numbers are based on the following assumptions:

- Hyper-threading is enabled in the ESXi compute nodes.
- There is no virtual CPU oversubscription. That is, the recommended number of virtual CPUs is the same as the number of actual physical cores.

These numbers include VMware overhead. You might need to adjust these numbers, based on your specific deployment.

VMP Service Manager GUI Requirements

The VMP Service Manager GUI can run on the following operating systems and browsers:

- Windows Internet Explorer 9 (IE9) or later for Windows 7
- Mozilla Firefox 20 or later for Windows 7
- Google Chrome 30.x for Windows 7
- Apple Safari 7.x for Windows 7 or MAC OS Version 10.9 or later

The VMP Service Manager GUI requires a display resolution of 1600 x 900 or better.

Restrictions and Limitations

- The VMP does not support IPv6.
- The image version for a node must match the image version configured in the associated software image manifest. For more information, see the Configuring VMP Nodes, page 78 and the Configuring Software Image Manifests, page 91.
- When you configure your network for HA redundancy, we recommend that you take the following considerations into account:
  - Place the redundant VMs and other appliances such that they are not fate-shared in terms of the availability of the ESXi server, the hardware, or the network.
  - Deploy the members of a given HA group on different blades, and ideally on different chassis.
  - Back up your databases at regular intervals.
- During streaming, do not use the **transaction-logs format** command to change the transaction log format (for example, from Extended Squid to Apache, or to a custom format).

Deploying the VMP

To deploy the VMP, perform the following tasks in order:

- Pre-Deployment Tasks, page 25
- Setting Up the External DNS Server, page 26
- Setting up the External Radius Server, page 29
- Deploying the VMP System, page 33
- Configuring the VMP Using the VMP Manager GUI, page 50

Pre-Deployment Tasks

Before deploying the VMP configuration, you must complete the following preliminary tasks:

Note: Virtual machine migration or cloning using the VMware infrastructure is not currently supported for any of the VMP nodes.

1. Prepare your VMP VMware datacenter topologies and networks. For more information, see Networks, page 5.
2. Download all of the VMP Open Virtual Appliance (OVA) files for local access.
3. Determine the blade and VM layout that you will use, and your IP address allocation scheme for the network interfaces.
4. Gather information related to Live feeds and multicast and unicast video sources and channels from the Cisco Digital Content Manager (DCM) or other sources. You will need this information when you create the channels and channel lineups in the VMP Service Manager GUI.
5. Install the external DNS and NTP servers for the playout clients.
   a. Determine the origin service FQDN and prepare the downstream client (client-facing) DNS servers to point to the IPVS dataplane (primary interface) IP addresses.

   Note: Wait until the MPE application comes up, then add the entries to the external DNS.

   b. Prepare the CDN-facing firewall. Load balancing for ODE playout is handled by the IPVS

   Note: Determine whether you require separate firewalls and DNS settings for origin services for Live and VOD playout. The administrator must ensure that the DNS zones are configured in the external DNS server and that the TCP and UDP ports 53 are accepted by the DNS server. Otherwise, the **nslookup** for **mgmt-docserver.***domain* fails and the PAM processes cannot begin. This problem can occur if you deploy a DNS server using Centos Linux distribution, which by default does not add a rule for UDP port 53. You can use the **iptables** command to set the correct firewall settings.

   The TTL for the DNS proxy requests is 1 second.
6. Prepare the NTP and key management servers on the Management network.
7. Prepare the NAS/COS stores and note the mount point, IP addresses, etc.

Setting Up the External DNS Server

VMP requires Linus DDNS. Dynamic entries are created and registered by the PAM. NTP on the DNS server must be synchronized with other VMP components.

Note: For VMP to work properly, the DNS setup should be redundant and protected from single point of failure.

Note: The following configuration is required if the DNS server starts automatically at boot-up.

```
In case of Centos 6 based OVA:
# chkconfig named on
In case of Centos 7 based OVA:
  # systemctl enable named
```

1. On the external DNS server, generate a TSIG key in one of the following algorithm formats: hmac-md5, hmac-sha1, hmac-sha224, hmac-sha256, hmac-sha384, and hmac-sha512.
2. Enter the following command:

```
dnssec-keygen -a HMAC-MD5 -b 128 -n HOST testdns.com.
```

where:

- **HMAC-MD5** is the TSIG algorithm.
- **128** is the number of bits in the key.
- **testdns.com.** is the name of the key. The name of the key, the domain name of the VMP, and the DNS zone in the external DNS server should all be the same (in this example, **testdns.com**).
- The command must end with a period (.), which is required when generating the key.

This command creates a .key file and a .private key file.

- Sample .key file:

```
Ktestdns.com.+157+05519.key
testdns.com. IN KEY 512 3 157 ujLdXfCZenQZQKZlFy42fw==
```

- Sample .private key file:

```
Ktestdns.com.+157+05519.private
\Private-key-format: v1.3
Algorithm: 157 (HMAC_MD5)
Key: ujLdXfCZenQZQKZlFy42fw==
Bits: AAA=
Created: 20140325141250
Publish: 20140325141250
Activate: 20140325141250
```

3. Create a new file called domain .key in the /etc/ directory and copy the TSIG key value from the .key file created previously. Press **“i”** to insert the following lines:

```
algorithm hmac-md5;
        secret “ujLdXfCZenQZQKZlFy42fw==“;
};
```

where:

- **hmac-md5** is the TSIG algorithm.
- **ujLdXfCZenQZQKZlFy42fw==** is the TSIG key.

4. Press **Ctrl-C** then :**wq** to save the file and exit.

5. Add the PAM IP (s) to the allow transfer line in /etc/named.conf
6. Press **"i"** to insert the following line:

```
allow-transfer /etc/testdns.com.key
```

7. Add the key file path to the file /etc/named.conf file.
8. Press **"i"** to insert the following lines then press **Ctrl-C** followed by **:wq** to save the file and exit.

```
include "/etc/testdns.com.key";
```

9. Add the forward and reverse zone names and file paths to the file /etc/named.conf (These files will be created /var/named/slaves/)
   - The DNS zone is related to the 172.20.216.xx subnet, which can be the Management interface.
   - For the Data In and Data Out interfaces, similar information related to the reverse zone must be added.
   - Data In is related to the 15.1.1.x subnet.
   - Data Out is related to the 25.1.1.x subnet.
   - **testdns.com.** is the key name.

```
DNS Zone Details
zone testdns.com IN {
type master;
file "slaves/db.testdns.com";
```

10. Press **"i"** to insert the following lines then press **Ctrl-C** followed by **:wq** to save the file and exit.

```
allow-update { key "testdns.com."; };
notify yes;
};
Reverse Zone Details (Management Interface)
zone 216.20.172.IN-ADDR.ARPA IN {
type master;
file "slaves/db.216.20.172";
allow-update { key "testdns.com."; };
notify yes;
};
Reverse Zone Details (Data In Interface)
zone 1.1.15.IN-ADDR.ARPA IN {
type master;
file "slaves/db.1.1.15";
allow-update { key "testdns.com."; };
notify yes;
};
Reverse Zone Details (Data Out Interface)
zone 1.1.25.IN-ADDR.ARPA IN {
type master;
file "slaves/db.1.1.25";
allow-update { key "testdns.com."; };
notify yes;
};
```

11. Create db.* files in the /var/named/slaves directory.
    a. A forward zone file and up to 4 reverse zone files must be created depending on the number of networks being deployed.

b. The filenames should match what was entered in the /etc/named.conf file.

Sample db File for DNS Zone (db.testdns.com)

```
$ORIGIN.
$TTL 86400 ; 1 day
testdns.com     IN SOA      dns.testdns.com. pam.testdns.com. (
                2014031009;serial
                3600;       refresh (1 hour)
                1800;       retry (30 minutes)
                604800;     expire (1 week)
                86400;      minimum (1 day)
            )
        NS  dns.testdns.com.
$ORIGIN testdns.com.
$TTL 1  ;1 second
$TTL 86400 ; 1 day
dhcp        CNAME   dns
dns         A   <IP address of your DNS server>
$TTL 86400 ; 1 day
ntp         CNAME   dns
```

Sample db File for Reverse Zone of Management Interface (db.216.20.172)

```
$ORIGIN .
$TTL 86400      ; 1 day
216.20.172.IN-ADDR.ARPA   IN SOA dns.testdns.com. pam.testdns.com. (
                                2012071021 ; serial
                                3600       ; refresh (1 hour)
                                1800       ; retry (30 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
                          NS      dns.testdns.com.
$ORIGIN 216.20.172.IN-ADDR.ARPA.
$TTL 7200       ; 2 hours
xx                      PTR     dns.testdns.com. //xx = last octet of the PAM IP
```

Sample db File for Reverse Zone for Data In Interface (db.1.1.15)

```
$ORIGIN .
$TTL 86400      ; 1 day
1.1.15.IN-ADDR.ARPA   IN SOA dns.testdns.com. pam.testdns.com. (
                                2012071021 ; serial
                                3600       ; refresh (1 hour)
                                1800       ; retry (30 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
                          NS      dns.testdns.com.
$ORIGIN 1.1.15.IN-ADDR.ARPA.
$TTL 7200       ; 2 hours
1                       PTR     dns.testdns.com.
```

Sample db File for Reverse Zone for Data Out Interface (db.1.1.25)

```
$ORIGIN .
$TTL 86400      ; 1 day
1.1.25.IN-ADDR.ARPA   IN SOA dns.testdns.com. pam.testdns.com. (
                                2012071021 ; serial
                                3600       ; refresh (1 hour)
                                1800       ; retry (30 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
                          NS      dns.testdns.com.
$ORIGIN 1.1.25.IN-ADDR.ARPA.
$TTL 7200       ; 2 hours
1                       PTR     dns.testdns.com.
```

12. Verify the DNS server is synchronized with NTP.

13. Restart DNS.

```
service named restart
```

Setting up the External Radius Server

The following procedure shows how to set the External Radius Server. The following is using FreeRADIUS as an example. To install FreeRadius and MYSQL:

```
# yum install mysql mysql-server
# yum install freeradius freeradius-mysql freeradius-utils
```

Start mysql

```
# service mysqld start
```

Create radius database:

```
# mysqladmin –u root create radius
```

Import radius schema to MYSQL

```
# mysql –u root radius < /etc/raddb/sql/mysql/admin.sql
# mysql –u root radius < /etc/raddb/sql/mysql/schema.sql
```

Update radius configuration with SQL option:

```
# vi /etc/raddb/radius.conf
Uncomment line
$INCLUDE sql.conf
# vi /etc/raddb/sites-enabled/default
Uncomment sql for authorize, accounting, session, and post-auth sections.
# vi /etc/raddb/sites-enabled/inner-tunnel
Uncomment sql for authorize, session, and post-auth sections.
```

Configure incoming clients:

```
# vi /etc/raddb/clients.conf

Add network configuration for the clients:
client 172.20.216.0/24 {
        secret = radius_secret
        shortname = test-network
}
```

Start radius:

```
# service radiusd restart
For throubleshooting radius can be started in debug mode with following command:
# radiusd -X
```

Add a test user:

```
# mysql –u radius radius
mysql>INSERT INTO radcheck(username, attribute, value, op) VALUES (‘testuser’, ‘Password’,
‘testuserpassword’, ’:=’);
mysql> exit;
```

Test radius service:

```
# radtest testuser testuserpassword localhost 1812 radius_secret
```

VMP Deployment Methodologies

VMP supports two deployment methodologies:

1. Cisco VMP OVA (referred to as the SuperOVA). The SuperOVA bundles all VM types into a single OVA. During SuperOVA deployment, the VM type personality is chosen.
2. RPM-based installation from a CentOS7 minimal OVA. RPM only requires the user to deploy a minimal CentOS7 OVA. Afterwards, a VMP installer script dynamically installs the desired VM type personality from an external yum Repository VM.

Cisco VMP SuperOVA

The Cisco VMP SuperOVA provides multiple service options (see list below) that can be chosen during the process of virtual machine deployment. The selection must be made during the SuperOVA deployment process.

- PAM service
- Common Logging Server (CLS) service
- Media Capture Engine (MCE) service
- App Engine (AE) service
- Media Playback Engine (MPE)

For the Common Logging Server (CLS), three storage sizes are available.

- 128 GB
- 256 GB
- 512 GB

The SuperOVA VM Types are listed below:

- VMP PAM
- VMP MCE
- VMP MPE
- VMP AE
- VMP Logger (Small VM)
- VMP Logger (Medium VM)
- VMP Logger (Large VM)

Note: To retrieve the version information for SuperOVA, run the following command.

```
rpm -q --info cisco-VMP-release
```

When deploying using the SuperOVA, all the VM types follow a common deployment flow (see list below). The only exception is the MPE OVA type which still uses the dedicated MPE OVA file.

- Deployment Configuration
- Map Networks
- Set up DNS/NTP Servers
- Authenticate Settings
- Set DNS/HA Credentials
- Set up Network Information

RPM-Based Deployment

The following section define the process to install the VMP App-group from a 2.6.0-centOS7 (minimal) OVA.

Software Images Required

1. 2.8.xxx-centos7-latest/2.8.xxx-cisco-VMP-centos7-mendocino.<buildNo>.ova

Note: Do *NOT* use the centos7.ova.

2. VMP Minimal Bootstrap RPM:
   2.8.xxx-cisco-VMP-mendocino-latest/cisco-VMP-minimal-bootstrap-2.8.xxx-<buildNo>.x86_64.rpm
3. REPO Bootstrap RPM:
   2.8.xxx-cisco-VMP-mendocino-latest/cisco-VMP-repo-bootstrap-2.8.xxx-<buildNo>.x86_64.rpm]
4. REPO ISO: 2.8.xxx-cisco-VMP-mendocino-latest/2.8.xxx-cisco-VMP-mendocino.<buildNo>.iso

OVF Properties Required

This is a sample script used to deploy and configure the 2.8.xxx-centos7 OVA using the OVF properties.

The OVF property values differ for each Test Bed deployment. This script is only given for reference.

```
#!/bin/bash -x
ovftool --noSSLVerify --powerOn --overwrite \
--name="pam1" \
--prop:"hostname=pam1" \
--prop:"domain=test1.com" \
--prop:"ip0=192.2.0.155" \
--prop:"subnet0=255.255.0.0" \
--prop:"gateway0=192.2.0.86"  \
--prop:"dns0=" \
--prop:"dns1=" \
--prop:"dns2=" \
--prop:"ntp0=192.2.0.86" \
--prop:"ntp1=1.1.1.1" \
--prop:"ntp2=2.2.2.2" \
--prop:ext-dns-ip=192.2.0.25 \
--prop:ext-dns-key=EA07/q61zERW7tziZupaUw== \
--prop:ext-dns-algo=hmac-md5 \
--datastore="datastore1" \
--acceptAllEulas \
--diskMode=thin \
--net:"Network for adapter 1"="net192" \
/sw/tools/2.8.xxx-cisco-VMP-centos7-mendocino.<buildNo>.ova \
vi://vCenterUser:vCenterPasswd@<vCenter-IP>/<DATACENTER/host/<HOST-IP>/
```

Test Bed SETUP Instructions

Setup a VMP Repository VM

In addition to the VMP setup requirements, the REPO VM is also needed.

1. Deploy the 2.8.xxx-centos7 OVA with the relevant OVF properties as shown above.
2. Copy the " REPO ISO" to /home/admin/
3. Copy the " REPO Bootstrap RPM" to /home/admin/
4. Install the VMP repo bootstrap rpm.

```
rpm -ivh cisco-VMP-repo-bootstrap-2.8.xxx-<buildnum>.x86_64.rpm
```

5. After installing the cisco-VMP-repo-bootstrap-2.8.xxx-<buildnum>.x86_64.rpm, the following file will exist:

```
etc/opt/cisco/VMP/repo/config.txt
```

The user should first edit this file as follows:

```
# vi /etc/opt/cisco/VMP/repo/config.txt
domain:<domain>
hostname:VMP-repo
hostIp:<VMPRepoHostIp>
dnsServerIp:<dnsServerIp>
ntpServerIp:<ntpServerIp>
tsigKey:<dnsTsigKey>
tsigAlgo:<dnsTsigAlgo
```

The user should then run the VMP Repo VM setup process:

```
/opt/cisco/VMP/repo/bin/VMP-repo-setup.sh /etc/opt/cisco/VMP/repo/config.txt
All initialization progress is logged to: /var/log/VMP-repo-setup.log.
```

6. Verify that the VMP-repo is setup correctly.
   - All initialization progress is logged to /var/log/VMP-repo-setup.log. When completed, VMP-repo-setup.sh will display the following messages:
   - (example shown for DNS server = 11.0.0.103, domain = test.com, hostIp = 11.0.0.51)
   - VMP DNS CONFIGURATION RESULTS:

     DNS server (11.0.0.103)

     Successfully updated with VMP-repo.test.com (11.0.0.51)

     Cisco VMP repo server setup complete!

```
Hosted repo URL: http://VMP-repo/VMP/repo/2.8.xxx/yumrepo
```

Deploying/Installing an App Group

1. Deploy the 2.8.xxx-centos7 OVA with the relevant OVF properties as shown above.
2. Copy the " VMP minimal Bootstrap RPM" to /home/admin/
3. Install the VMP minimal bootstrap rpm

```
rpm -ivh cisco-VMP-minimal-bootstrap-2.8.xxx-<buildnum>.x86_64.rpm
```

4. Execute the command shown below.

```
/opt/cisco/VMP/bootstrap/bin/VMP_install.sh <pam-app | logger-app | appengine | mpe-app | mce-app>
```

If installing the PAM, use the pam-app option. The above command is a blocking command. It will not return until pam-app is installed.

Output from the command is logged in the log file shown below:

```
/var/log/VMP-app-install.log
```

5. Verify the application is installed correctly.

```
#service pam-app status
#supervisorctl status
```

Deploying the VMP System

To fully deploy the Platform and Applications Manager (PAM)/VMP System, perform the following tasks in order:

- Setting Up the CLS, page 33
- Deploying the PAM HA, page 34
- UCS Configuration, page 37
- Setting Up the MCE, page 39
- Setting Up the MPE, page 41
- Setting Up the App Engine, page 44

When deploying the PAM/VMP System, keep the following considerations in mind:

- Deployment requires VMware vCenter version 5.1 or later.
- If you need to upgrade the PAM to a new OVA, you must disable or deactivate all of the services that you have configured in the PAM before performing the upgrade.

Setting Up the CLS

Before Setting up the CLS, refer to the Cisco VMP SuperOVA, page 30.

Deploy the Centralized Log Server (CLS) from vCenter.

1. Log into the vCenter.
2. From the **File** menu, select **Deploy OVF Template**, then select the Cisco VMP OVA file.
3. Choose the required CLS OVA type with the appropriate disk size from the drop-down menu.
4. Accept the license agreement.
5. Select Network Mapping and map **Network Adapter 1** to the Management network. **Network Adapter 1** must always map to the Management network, and CLS VM applications use only **Network Adapter 1**. The other network adapters are ignored; it does not matter what they are mapped to.
6. Select Properties to customize the VM deployment.
7. In the Networking section, enter the following information to customize:

- Domain—Domain name used by the CLS (required). Enter the same domain name used by the PAM.
- IP Address—IP address for Network Adapter 1 (required).
- Subnet Mask—Subnet mask for Network Adapter 1 (required).
- Gateway—Gateway IP address for Network Adapter 1 (required).
- Primary DNS Server—Name or IP address of the DNS server used by the CLS to forward queries that it could not resolve (that is, the DNS forwarder). Enter names for all of the DNS servers used by the CLS.
- You must enter at least one DNS server.
- Primary NTP Server—Name or IP address of the external Network Time Protocol (NTP) server used by the CLS to synchronize its clock. Enter names for all of the NTP servers used by the CLS.
- You must enter at least one NTP server.
- Hostname: Please enter exactly "log-server". Do not specify the fully qualified domain name (FQDN).

8. In the External DNS Credentials section, enter the following information:
   - DNS Server—Name or IP address of the external DNS server used by the CLS to forward queries that it could not resolve.
   - Transaction Signature Key—Transaction Signature (TSIG) key that is configured on the external DNS server.
   - Transaction Signature Algorithm—Name of the TSIG algorithm that is configured on the external DNS server.

Note: The administrator must ensure that the DNS zones are configured in the external DNS server and ensure that TCP and UDP ports 53 are accepted by the DNS server. Otherwise, the **nslookup** for **mgmt-docserver.***domain* fails and the CLS processes cannot begin. This problem can occur if you deploy a DNS server using Centos Linux distribution, which by default does not add a rule for UDP port 53. You can use the **iptables** command to set the correct firewall settings.

9. Click **Finish** to deploy the OVA and create the CLS VM. It can take up to 15 minutes to create the VM.
10. After mapping the adapter to the correct network, power on the CLS VM.
11. Verify connectivity and open an SSH into the CLS VM.

Logging into the CLS VM

After deployment, if you need to log in to the CLS VM, log in as "**admin/default**".

Changing the OVF Properties After Deployment

If you need to change any of the OVF properties after deploying the CLS VM, use the following procedure:

1. Power off the CLS VM.
2. Change the properties in vCenter.
3. Power on the CLS VM.

An **admin** user cannot directly change the guest OS configuration files that are driven by any of the OVF properties upon boot up.

Deploying the PAM HA

To deploy the PAM HA, perform the following tasks in order:

- Pre-Deployment Tasks for PAM HA, page 35

- Setting Up the PAMs for HA, page 35

Pre-Deployment Tasks for PAM HA

Note: These HA-specific pre-deployment tasks must be performed **in addition to** the tasks specified in the Pre-Deployment Tasks, page 25. These tasks supplement those tasks, they do not replace them.

Before deploying the VMP configuration, you must complete the following preliminary tasks:

1. Determine the IP addresses for each of the PAM HA nodes. You will need these IP addresses when you configure the High-Availability section of the OVF properties. (See Step 6 in Setting Up the PAMs for HA, page 35.)
2. Set up a DNS server for the PAM HA domain. You will need the name or IP address of this DNS server when you configure the External DNS Credentials section of the OVF properties. (See Step 9 in Setting Up the PAMs for HA, page 35.)

Make sure the DNS zones are configured in the DNS server.

Setting Up the PAMs for HA

Deploy each of the PAM HA nodes from vCenter.

1. Log into the vCenter.
2. From the **File** menu, select **Deploy OVF Template**, then select the Cisco VMP OVA file.
3. Choose the required PAM OVA type (VMP PAM) from the drop-down menu.
4. Accept the license agreement.
5. In the Deploy OVF Template field, select Network Mapping and map **Network Adapter 1** to the Management network. **Network Adapter 1** must always map to the Management network, and PAM VM applications use only **Network Adapter 1**.
6. Select Properties to customize the VM deployment.
7. In the Networking section, enter the following information to customize:
   - Hostname—Local hostname of the PAM. Do not enter the fully qualified domain name (FQDN). For example, if the FQDN is pam.cisco.com, enter only **pam**.
   - Domain—Domain name used by the PAM, such as **testdns.com** (required).
   - IP Address—Primary management IP address to which the VMP can SSH (required). This is the IP address for the Management network for the PAM and for configuring Ethernet port eth0. The management IP address must be accessible from a management PC (for example, from a PC that is running vSphere).
   - Subnet Mask—Default subnet mask for the PAM (required).
   - Gateway—Default gateway IP address for the PAM (required).
8. In the High-Availability section, enter the following information:
   - High-Availability Peer—Enter the IP addresses of the peer PAM HA nodes.

   For example, given three PAM HA nodes with IP addresses 35.1.2.50, 35.1.2.51, and 35.1.2.52, if this PAM HA node uses IP address **35.1.2.50**, enter **35.1.2.51** in the first High-Availability Peer field and enter **35.1.2.52** in the second High-Availability Peer field.
9. In the Additional Domain Name Servers section, enter the following information:

- DNS Server—Name or IP address of the DNS server used by the PAM to forward queries that it could not resolve (that is, the DNS forwarder). Enter names for all of the DNS servers used by the PAM.

10. In the Additional Network Time Protocol Servers section, enter the following information:

    - NTP Server—Name or IP address of the external Network Time Protocol (NTP) server used by the PAM to synchronize its clock. Enter names for all of the NTP servers used by the PAM.

    You must enter at least one NTP server.

11. If you choose to use Radius as your authentication point, you must set your authentication settings, ie server IP name and server secret password. If not set, the server will use the local authentication only. You can also specify the password (default) for the local admin user.

12. In the External DNS Credentials section, enter or select the following information:

- DNS Server—Name or IP address of the external DNS server used by the PAM to forward queries that it could not resolve. This is the DNS server for the PAM HA domain that you set up in Step 2 of the Pre-Deployment Tasks for PAM HA, page 35.)

  Note: The administrator must ensure that the DNS zones are configured in the external DNS server.

- Transaction Signature Key—Transaction Signature (TSIG) key that is configured on the external DNS server.

- Transaction Signature Algorithm—Name of the TSIG algorithm that is configured on the external DNS server. Valid TSIG algorithms are:

  - hmac-md5
  - hmac-sha1
  - hmac-sha224
  - hmac-sha256
  - hmac-sha384
  - hmac-sha512

13. Click **Finish** to deploy the OVA and create the PAM VM. It can take up to 15 minutes to create the VM.

14. After mapping the adapter to the correct network, power on the PAM VM.

15. Verify connectivity and open an SSH into the PAM VM.

16. Repeat this entire procedure for each of the peer PAM HA nodes.

When all of the PAM HA nodes are fully deployed, HA is set up and is running.

Logging into the PAM VM

After deployment, if you use Radius authentication, you can log in to the PAM VM using the default username **admin** and the password you specified on the Radius server. If you use non-Radius authentication, use the password **default or your local admin user password.** After logging in, you can change the password as you would any other Linux password.

This default user account can perform the normal Linux user functions, and it also provides the following limited root privileges, so that you can perform necessary maintenance and troubleshooting on the PAM VM:

- Networking commands, such as **/sbin/iptables**, **/sbin/route**, and **/sbin/dhclient**, that enable you to troubleshoot problems, maintain networking functionality, and keep the PAM operating normally.

- Software maintenance commands, such as **/bin/rpm**, **/usr/bin/up2date**, and **/usr/bin/yum**, that enable you to upgrade the PAM software as needed.

- Commands for rebooting and shutting down the PAM VM, such as **reboot** and **shutdown now**.

If you need to upgrade the PAM CLI, log in as **admin**, upgrade the software, and either reboot the PAM VM or use the **supervisorctl** command to restart all of the processes.

If you need to troubleshoot a problem because the PAM CLI is not operating normally, log in as the **admin** and examine all relevant logs to determine the problem. If needed, you can **scp** the log files from the PAM VM and send them to Cisco support for further analysis.

Changing the OVF Properties After Deployment

If you need to change any of the OVF properties after deploying the PAM VM, use the following procedure:

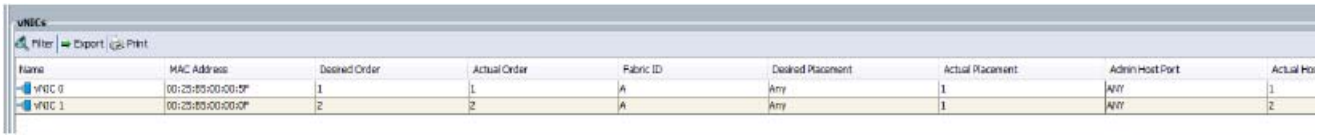
1. Power off the PAM VM.
2. Change the properties in vCenter.
3. Power on the PAM VM.

An **admin** user cannot directly change the guest OS configuration files that are driven by any of the OVF properties upon boot up.

UCS Configuration

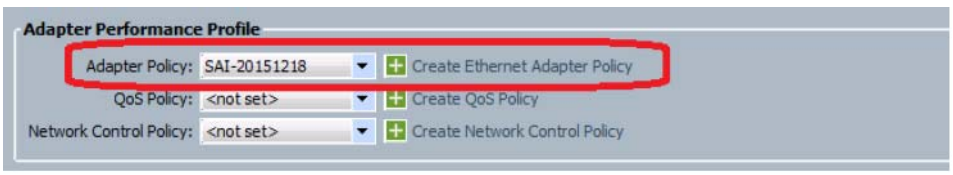
To optimize the traffic flow through the MCE Workers, changes are required at the UCS and ESXi infrastructure level. The lowest level, UCS, must be configured first. Follow the instructions below.

1. Create two vNICs on the UCS Server.

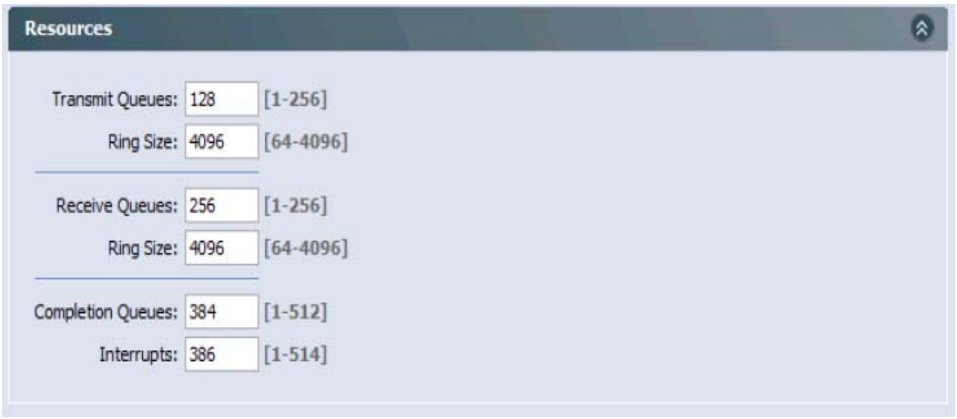


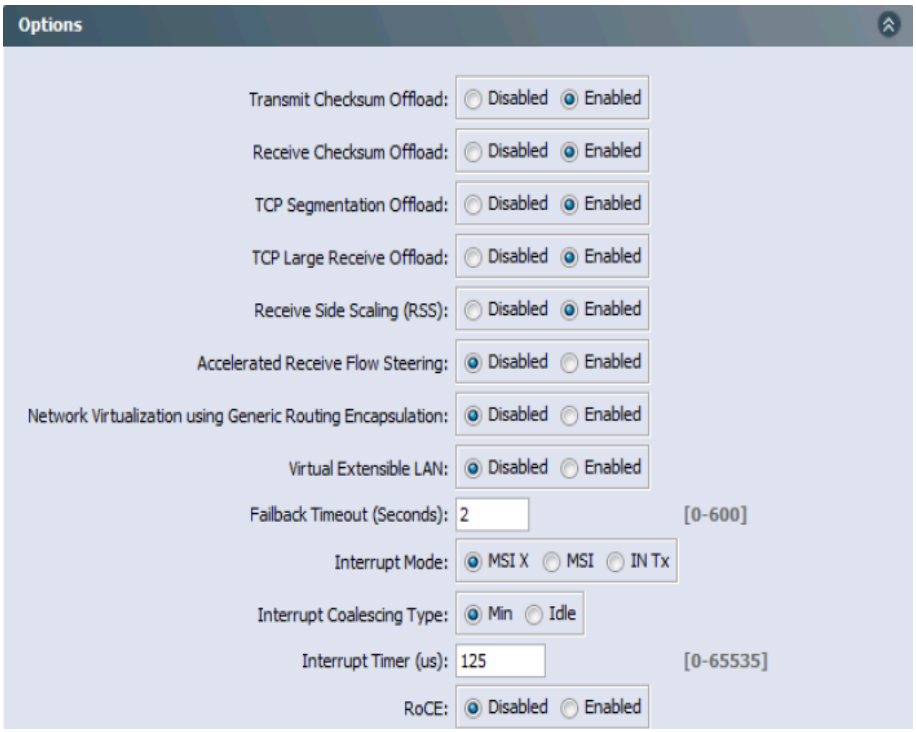
If you have an HA system with dual UCS FI's, configure the fabric failover in the Fabric ID field. In this example, it is a non-HA configuration. Configure each vNIC as you normally would but be sure to enable the Management and Data-In VLANS on vNIC0 and Data-Out VLAN on VNIC1. You can enable all VLANs on both, as the ESXi settings will route to the appropriate VLAN.

2. On the Adapter Performance Profile menu, click "Create Ethernet Adapter Policy".



3. Configure the policy as shown in the screens below.



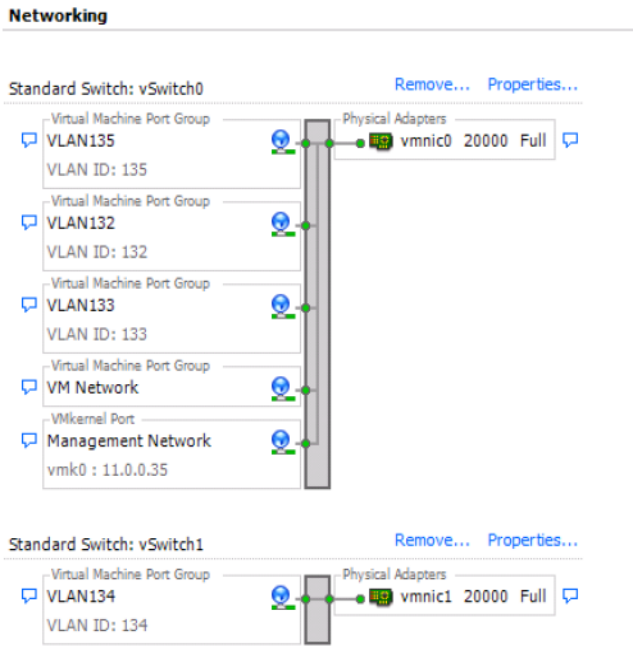


4. Assign the policy to both adapters. This will cause the blade to reboot. After the blade comes back up, configure the Security profile to enable ESXi Shell and SSH. Once complete, start an SSH session to the ESXi server IP address and execute the following commands:
   - esxcli system settings advanced set-o “Net/MaxPktRxListQueue” -i 15000
   - esxcli system settings advanced set-o “Net/MaxNetifTxQueueLen” -i 10000
   - esxcli system settings advanced set-o “Net/MaxNetifRxQueueLen” -i 1000
   - esxcli system settings advanced list -d

Note: The last command is used to show that the previous commands were set properly. Reboot the server for these changes to take place.

5. During OVA deployment, the vNIC's should be allocated as follows: In this case, the Management and Data-In VLANs should be configured to vNIC0 and Data-Out VLAN configured to vNIC1. Add a second vSwitch (a running ESXi node typically has a vSwitch0 already configured). If you have previously assigned the Data-Out VLAN to vSwitch0, remove this setting. Add the second vSwitch (vSwitch1) and assign the Data-Out VLAN to that vSwitch.

6. Deploy your OVA as before and ensure the allocations are correctly mapped to the right vNICs. It should look something like this:



Setting Up the MCE

Deploy each Media Capture Engine (MCE) from the Cisco VMP OVA file.

Note: The MCE does not support changing a storage location during capturing and playback for Live, VOD and cDVR use cases.

1. Log in to vCenter.
2. From the **File** menu, select **Deploy OVF Template**, then select the MCE OVA file.
3. Accept the license agreement.
4. In the Deploy OVF Template field, select Network Mapping to map the source networks to the destination networks. MCE VM applications use up to three network adapters, but **Network Adapter 1** must always map to the Management network:
   - If you are using only one network adapter, map **Network Adapter 1** to the Management network.
   - If you are using two network adapters, use one of the following connection schemes, depending on your preferred topology:
   - Connect **Network Adapter 1** to the Management network and **Network Adapter 2** to the Data In and Data Out networks.

  - Connect **Network Adapter 1** to the Management and Data In networks and **Network Adapter 2** to the Data Out networks.
  - Connect **Network Adapter 1** to the Management and Data Out networks and **Network Adapter 2** to the Data In networks.

- If you are using three network adapters:
  - Connect **Network Adapter 1** to the Management network.
  - Connect **Network Adapter 2** to the Data In network.
  - Connect **Network Adapter 3** to the Data Out network.

5. Select Properties to customize the VM deployment.
6. In the Network Parameters section, enter the following information to customize:
   - Hostname—Local hostname of the MCE. Do not enter the fully qualified domain name (FQDN). For example, if the FQDN is mce.cisco.com, enter only **mce**.
   - Domain—Domain name used by the MCE (required). Enter the same domain name used by the PAM.
   - IP Address—IP address for Network Adapter 1 (required).
   - Subnet Mask—Subnet mask for Network Adapter 1 (required).
   - Gateway—Gateway IP address for Network Adapter 1 (required).
7. In the Additional Domain Name Servers section, enter the following information:
   - DNS Server—Use the external DNS
8. In the Additional Network Time Protocol Servers section, enter the following information:
   - NTP Server— Use the external NTP
9. Click **Finish** to deploy the OVA and create the MCE VM. It can take up to 15 minutes to create the VM.
10. Power on the MCE VM.
11. Verify connectivity and open an SSH into the MCE VM.
12. To manually add a second Ethernet interface, as dictated by your network topology, log in as **admin** (see the Logging into the MCE VM, page 41), then create and save the /etc/sysconfig/network-scripts/ifcfg-eth1 file with contents like those in the following example:

```
TYPE=Ethernet
NAME=eth1
DEVICE=eth1
BROADCAST=11.0.0.255      < Broadcast address of your interface
IPADDR=11.0.0.xx          < IP address of your interface
NETMASK=255.255.255.0     < Netmask of your interface
NETWORK=11.0.0.0          < Network address of your interface
USERCTL=no
BOOTPROTO=none
ONBOOT=yes
HWADDR=00:50:56:AC:7D:4C
```

Do not include a GATEWAY for this interface.

Note: All MCE and MPE nodes in a region that use the same Image Type, Image Version, and Personality must have identical route configurations. For more information, see Configuring VMP Nodes, page 78.

13. If you need to route specific traffic to and from this interface, you must add one or more static routes. To do so, create and save the /etc/sysconfig/network-scripts/route-eth1 file with contents like those in the following example:

```
ADDRESS0=10.1.2.44        < Routed IP address
GATEWAY0=10.1.1.1         < Gateway to the route to and from this interface
NETMASK0=255.255.255.0    < Netmask for routed IP address
```

You can add as many additional static routes as you need. To do so, add additional lines for ADDRESS1/GATEWAY1/NETMASK1; ADDRESS2/GATEWAY2/NETMASK2; and so on.

14. Bring up eth1 using the **`sudo ifup eth1`** command.

15. To manually add a third Ethernet interface, create and save the /etc/sysconfig/network-scripts/ifcfg-eth2 file, and repeat step 11 through 13. Remember to specify **eth2** as the Name and Device, specify the IP addresses of the eth2 interface, and use the **`sudo ifup eth2`** command to bring up eth2.

Logging into the MCE VM

After deployment, you can log in to the MCE VM using the default username **admin** and the default password **default**. After logging in, you can change the password as you would any other Linux password.

This default user account can perform the normal Linux user functions, and it also provides the following limited root privileges, so that you can perform necessary maintenance and troubleshooting on the MCE VM:

- Networking commands, such as **/sbin/iptables**, **/sbin/route**, and **/sbin/dhclient**, that enable you to troubleshoot problems, maintain networking functionality, and keep the MCE operating normally.
- Software maintenance commands, such as **/bin/rpm**, **/usr/bin/up2date**, and **/usr/bin/yum**, that enable you to upgrade the MCE software as needed.
- Commands for rebooting and shutting down the MCE VM, such as **reboot** and **shutdown now**.

If you need to upgrade the MCE CLI, log in as **admin**, upgrade the software, and either reboot the MCE VM or use the **supervisorctl** command to restart all of the processes.

If you need to troubleshoot a problem because the MCE CLI is not operating normally, log in as the **admin** and examine all relevant logs to determine the problem. If needed, you can **scp** the log files from the MCE VM and send them to Cisco support for further analysis.

Changing the OVF Properties After Deployment

If you need to change any of the OVF properties after deploying the MCE VM, use the following procedure:

1. Power off the MCE VM.
2. Change the properties in vCenter.
3. Power on the MCE VM.

An **admin** user cannot directly change the guest OS configuration files that are driven by any of the OVF properties upon boot up.

Setting Up the MPE

Deploy each MPE from the Cisco VMP OVA file.

1. From the **File** menu, select **Deploy OVF Template**, then select the VMP MPE OVA file.
2. Accept the license agreement.
3. In the Deployment Configuration, choose the VMP MPE type.

4. In the Deploy OVF Template field, select **Network Mapping** to map the source networks to the destination networks. MPE VM applications use up to three network adapters, but Network Adapter 1 must always map to the Management network:
   a. If you are using only one network adapter, map Network Adapter 1 to the Management network.
   b. If you are using two network adapters, use one of the following connection schemes, depending on your preferred topology:
   c. Connect Network Adapter 1 to the Management network and Network Adapter 2 to the Data In and Data Out networks.
   d. Connect Network Adapter 1 to the Management and Data In networks and Network Adapter 2 to the Data Out networks.
   e. Connect Network Adapter 1 to the Management and Data Out networks and Network Adapter 2 to the Data In networks.

If you are using three network adapters:

   a. – Connect **Network Adapter 1** to the Management network.
   b. – Connect **Network Adapter 2** to the Data In network.
   c. – Connect **Network Adapter 3** to the Data Out network.

5. Select Properties to customize the VM deployment.
   a. In the Network Parameters section, enter the following information:
   b. – Hostname–Local hostname of the MCE. Do not enter the fully qualified domain name (FQDN). For example, if the FQDN is mce.cisco.com, enter only mce.
   c. – Domain–Domain name used by the MCE (required). Enter the same domain name used by the PAM.
   d. – IP Address–IP address for Network Adapter 1 (required).
   e. – Subnet Mask–Subnet mask for Network Adapter 1 (required).
   f. – Gateway–Gateway IP address for Network Adapter 1 (required).
6. In the Additional Domain Name Servers section, enter the following information:
   a. – DNS Server–Use the external DNS
7. In the Additional Network Time Protocol Servers section, enter the following information:

– NTP Server– Use the external NTP

8. Click **Finish** to deploy the OVA and create the MPE VM. It can take up to 15 minutes to create the VM.
9. Power on the MPE VM.
10. Verify connectivity and open an SSH into the MPE VM.
11. To manually add a second Ethernet interface, as dictated by your network topology, log in as admin (see the Logging into the MCE VM, page 41), then create and save the /etc/sysconfig/network-scripts/ifcfg-eth1 file with contents like those in the following example:

```
TYPE=Ethernet
NAME=eth1
DEVICE=eth1
BROADCAST=11.0.0.255
IPADDR=11.0.0.xx
```

```
NETMASK=255.255.255.0
NETWORK=11.0.0.0
USERCTL=no
BOOTPROTO=none
ONBOOT=yes
HWADDR=00:50:56:AC:7D:4C
< Broadcast address of your interface
< IP address of your interface
ADDRESS0=10.1.2.44
GATEWAY0=10.1.1.1
NETMASK0=255.255.255.0
< Routed IP address
< Gateway to the route to and from this interface
< Netmask for routed IP address
< Netmask
< Network
of your interface
address of your interface
```

Do not include a GATEWAY for this interface.

Note: All MCE and MPE nodes in a region that use the same Image Type, Image Version, and Personality must have identical route configurations. For more information, see Configuring VMP Nodes, page 78

12. If you need to route specific traffic to and from this interface, you must add one or more static routes. To do so, create and save the /etc/sysconfig/network-scripts/route-eth1 file with contents like those in the following example: You can add as many additional static routes as you need. To do so, add additional lines for ADDRESS1/GATEWAY1/NETMASK1; ADDRESS2/GATEWAY2/NETMASK2; and so on.
13. Bring up eth1 using the sudo ifup eth1 command.
14. To manually add a third Ethernet interface, create and save the /etc/sysconfig/network-scripts/ifcfg-eth2 file, and repeat steps 11 through 13. Remember to specify eth2 as the Name and Device, specify the IP addresses of the eth2 interface, and use the **sudo ifup eth2** command to bring up eth2.

Logging into the MPE VM

After deployment, you can log in to the MPE VM using the default username **admin** and the default password **default**. After logging in, you can change the password as you would any other Linux password.

This default user account can perform the normal Linux user functions, and it also provides the following limited root privileges, so that you can perform necessary maintenance and troubleshooting on the MPE VM:

- Networking commands, such as **/sbin/iptables**, **/sbin/route**, and **/sbin/dhclient**, that enable you to troubleshoot problems, maintain networking functionality, and keep the MCE operating normally.
- Software maintenance commands, such as **/bin/rpm**, **/usr/bin/up2date**, and **/usr/bin/yum**, that enable you to upgrade the MCE software as needed.
- Commands for rebooting and shutting down the MCE VM, such as **reboot** and **shutdown now**. If you need to upgrade the MCE CLI, log in as **admin**, upgrade the software, and either reboot the MCE VM or use the **supervisorctl** command to restart all of the processes.

If you need to troubleshoot a problem because the MPE CLI is not operating normally, log in as the **admin** and examine all relevant logs to determine the problem. If needed, you can **scp** the log files from the MCE VM and send them to Cisco support for further analysis.

Changing the OVF Properties After Deployment

If you need to change any of the OVF properties after deploying the MCE VM, use the following procedure:

a. Power off the MCE VM.

b. Change the properties in vCenter.

c. Power on the MCE VM. An **admin** user cannot directly change the guest OS configuration files that are driven by any of the OVF properties upon boot up.

15. Login to the MPE and run the supervisorctl status command. Check to make sure the ServiceAgent and trafficserver is RUNNING. See below command sample.

```
[admin@mpe-138 ~]$ supervisorctl status
ServiceAgent                     RUNNING   pid 10681, uptime 2 days, 1:06:45
StorageMain                      RUNNING   pid 3006, uptime 14 days, 11:52:04
mpe-initscript                   STOPPED Not started
trafficserver                    RUNNING   pid 27068, uptime 10:24:43

StorageMain: stopped
ServiceAgent: stopped
trafficserver: stopped
mpe-initscript: started
StorageMain: started
ServiceAgent: started
trafficserver: started
```

MPE log info:

For MPE specific logs, go to /var/log/opt/cisco/VMP/cts, there are diags.log ingest.log, error.log, squild.log, traffic.out.

Setting Up the App Engine

Introduction

The AppEngine nodes serve as the IPVS node for MCE/MPE to implement load balance. By default, the DR (direct routing) mode is used for forwarding. The DR mode requires all machines (the director and real servers) to be on the same segment. There must be no forwarding devices between them.

In some deployment scenarios, App Engine nodes may be deployed in a different network from the MCE/MPE's network. If these App Engine nodes serve as IPVS director for MCE/MPE, the DR forwarding will not work.

To solve this issue, these App Engine nodes can be tagged and assigned a node allocation mechanism based on the tag. For example, the App Engine nodes within the MPE's network can be tagged with the " smplaybackep" attribute. Only tagged App Engine nodes are candidates for IPVS node for MPE nodes.

Follow the configuration instructions below.

1. Tag the AppEngine Nodes

Users should tag the AppEngine node to restrict its assignment:

smcaptureep : to restrict its assignment to MCE

smplaybackep : to restrict its assignment to MPE

Note: Tagging can be done through the RESTful API or GUI. If tagging from the GUI, select the AIC type for playback as MPE and capture as MCE.

a. Register node through RESTful API

```
#>vi nodex.json
           {
               "name":"VMPa-ae-27",
               "properties":{
                   "image":{"imgTag":"appengine","personality":"worker","version":"2.4"},
                   "description":"",
```

```
                    "adminState":"maintenance",
                    "zoneRef":"smtenant_system.smzone.zone-1",
                    "aic":"smplaybackep",
                    "interfaces":[
                        {"type":"data-in","inet":"192.168.1.27"},
                        {"type":"data-out","inet":"192.168.1.27"},
                        {"type":"mgmt","inet":"192.168.1.27"}
                    ]
                }
            }
            // "aic":"smplaybackep",  the AppEngine node is supposed to be assigned as IPVS node for
MPE


            #>curl -k -u admin:default -X POST -d @nodex.json -H "Accept: application/json" -H
"Content-Type: application/json"

https://10.74.14.113:8043/v2/regions/region-0/nodes/VMPa-ae-27
```

b. Modify node through RESTful API

```
 #>vi nodex.json
            {
                "name":"VMPa-ae-27",
                "properties":{
                    "image":{"imgTag":"appengine","personality":"worker","version":"2.4"},
                    "description":"",
                    "adminState":"maintenance",
                    "zoneRef":"smtenant_system.smzone.zone-1",
                    "aic":"smplaybackep",
                    "interfaces":[
                        {"type":"data-in","inet":"192.168.1.27"},
                        {"type":"data-out","inet":"192.168.1.27"},
                        {"type":"mgmt","inet":"192.168.1.27"}
                    ]
```

c. Put the node in maintenance mode.

```
            #>curl -k -u admin:default -X PUT -d @nodex.json -H "Accept: application/json" -H
"Content-Type: application/json"

https://10.74.14.113:8043/v2/regions/region-0/nodes/VMPa-ae-27
```

d. put node in inservice

2. Configure the Node Allocation Strategy.

Note: All operations are supposed to be done at the PAM node.

a. create the following config file:

```
 #>vi /etc/opt/cisco/VMP/VMP.cfg
            {
                "node": {
                    "allocator": "insVmAllocator.NodeAllocator4IPVS"
                }
            }
```

b. If you want to allocate node regardless of the tag, you can revert allocator attribute to:

```
"insVmAllocator.NodeAllocator";
```

c. To keep backward compatibility, you can simply remove the following file to use the default node allocation mechanism.

```
 #>vi etc/opt/cisco/VMP/VMP.cfg
```

```
{
    "node": {
        "allocator": "insVmAllocator.NodeAllocator"
    }
}
```

3. After modifing the VMP.cfg file, restart pam-installedVm process to apply the configuration.

```
#>supervisorctl restart pam-installedVm
```

Deploy Each App Engine from the Cisco VMP OVA File

1. Log in to the vCenter.
2. From the **File** menu, select **Deploy OVF Template**, then select the App engine OVA file.
3. Accept the license agreement.
4. In the Deploy OVF Template field, select Network Mapping to map the source networks to the destination networks. App Engine VM applications use up to three network adapters, but **Network Adapter 1** must always map to the Management network:

- If you are using only one network adapter, map **Network Adapter 1** to the Management network.
- If you are using two network adapters, use one of the following connection schemes, depending on your preferred topology:
  - Connect **Network Adapter 1** to the Management network and **Network Adapter 2** to the Data In and Data Out networks.
  - Connect **Network Adapter 1** to the Management and Data In networks and **Network Adapter 2** to the Data Out networks.
  - Connect **Network Adapter 1** to the Management and Data Out networks and **Network Adapter 2** to the Data In networks.
- If you are using three network adapters:
  - Connect **Network Adapter 1** to the Management network.
  - Connect **Network Adapter 2** to the Data In network.
  - Connect **Network Adapter 3** to the Data Out network.

5. Select Properties to customize the VM deployment.
6. In the Network Parameters section, enter the following information to customize:
   - Hostname—Local hostname of the App Engine. Do not enter the fully qualified domain name (FQDN). For example, if the FQDN is ae.cisco.com, enter only **ae**.
   - Domain—Domain name used by the App Engine (required). Enter the same domain name used by the PAM.
   - IP Address—IP address for Network Adapter 1 (required).
   - Subnet Mask—Subnet mask for Network Adapter 1 (required).
   - Gateway—Gateway IP address for Network Adapter 1 (required).
7. In the Additional Domain Name Servers section, enter the following information:
   - DNS Server—Use the external DNS

8. In the Additional Network Time Protocol Servers section, enter the following information:
   - NTP Server– Use the external NTP
9. Click **Finish** to deploy the OVA and create the App Engine VM. It can take up to 15 minutes to create the VM.
10. Power on the App Engine VM.
11. Verify connectivity and open an SSH into the App Engine VM.
12. To manually add a second Ethernet interface, as dictated by your network topology, log in as **admin** (see the Logging into the App Engine VM, page 47), then create and save the /etc/sysconfig/network-scripts/ifcfg-eth1 file with contents like those in the following example:

```
TYPE=Ethernet
NAME=eth1
DEVICE=eth1
BROADCAST=11.0.0.255       < Broadcast address of your interface
IPADDR=11.0.0.xx           < IP address of your interface
NETMASK=255.255.255.0      < Netmask of your interface
NETWORK=11.0.0.0           < Network address of your interface
USERCTL=no
BOOTPROTO=none
ONBOOT=yes
HWADDR=00:50:56:AC:7D:4C
```

Do not include a GATEWAY for this interface.

Note: All App Engine and AE nodes in a region that use the same Image Type, Image Version, and Personality must have identical route configurations. For more information, see the Configuring VMP Nodes, page 78.

13. If you need to route specific traffic to and from this interface, you must add one or more static routes. To do so, create and save the /etc/sysconfig/network-scripts/route-eth1 file with contents like those in the following example:

```
ADDRESS0=10.1.2.44         < Routed IP address
GATEWAY0=10.1.1.1          < Gateway to the route to and from this interface
NETMASK0=255.255.255.0     < Netmask for routed IP address
```

You can add as many additional static routes as you need. To do so, add additional lines for ADDRESS1/GATEWAY1/NETMASK1; ADDRESS2/GATEWAY2/NETMASK2; and so on.

14. Bring up eth1 using the **`sudo ifup eth1`** command.
15. To manually add a third Ethernet interface, create and save the /etc/sysconfig/network-scripts/ifcfg-eth2 file, and repeat 11 through 13. Remember to specify **eth2** as the Name and Device, specify the IP addresses of the eth2 interface, and use the **`sudo ifup eth2`** command to bring up eth2.

Logging into the App Engine VM

After deployment, you can log in to the App Engine VM using the default username **admin** and the default password **default**. After logging in, you can change the password as you would any other Linux password.

This default user account can perform the normal Linux user functions, and it also provides the following limited root privileges, so that you can perform necessary maintenance and troubleshooting on the App Engine VM:

- Networking commands, such as **/sbin/iptables**, **/sbin/route**, and **/sbin/dhclient**, that enable you to troubleshoot problems, maintain networking functionality, and keep the App Engine operating normally.
- Software maintenance commands, such as **/bin/rpm**, **/usr/bin/up2date**, and **/usr/bin/yum**, that enable you to upgrade the App Engine software as needed.

- Commands for rebooting and shutting down the App engine VM, such as **reboot** and **shutdown now**.

If you need to upgrade the App Engine CLI, log in as **admin**, upgrade the software, and either reboot the App Engine VM or use the **supervisorctl** command to restart all of the processes.

If you need to troubleshoot a problem because the App Engine CLI is not operating normally, log in as the **admin** and examine all relevant logs to determine the problem. If needed, you can **scp** the log files from the App Engine VM and send them to Cisco support for further analysis.

Changing the OVF Properties After Deployment

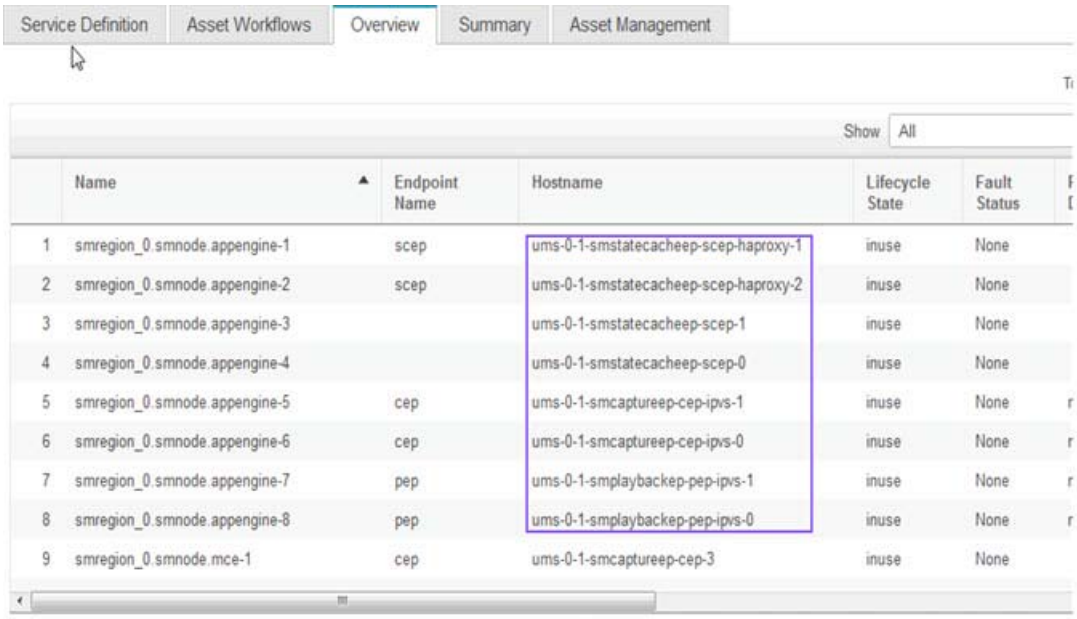
If you need to change any of the OVF properties after deploying the MCE VM, use the following procedure:

1. Power off the App Engine VM.
2. Change the properties in vCenter.
3. Power on the App EngineVM.

An **admin** user cannot directly change the guest OS configuration files that are driven by any of the OVF properties upon boot up.

App Engine Roles/ Descriptions

VMP defines the role of each App Engine (i.e IPVS, HA Proxy, or Redis) once the service has been enabled. See screen below. MCE IPVS = cep-ipvs, MPE IPVS = pep-ipvs, etc.



	Name	Endpoint Name	Hostname	Lifecycle State	Fault Status
1	smregion_0.smnode.appengine-1	scep	ums-0-1-smstatecacheep-scep-haproxy-1	inuse	None
2	smregion_0.smnode.appengine-2	scep	ums-0-1-smstatecacheep-scep-haproxy-2	inuse	None
3	smregion_0.smnode.appengine-3		ums-0-1-smstatecacheep-scep-1	inuse	None
4	smregion_0.smnode.appengine-4		ums-0-1-smstatecacheep-scep-0	inuse	None
5	smregion_0.smnode.appengine-5	cep	ums-0-1-smcaptureep-cep-ipvs-1	inuse	None
6	smregion_0.smnode.appengine-6	cep	ums-0-1-smcaptureep-cep-ipvs-0	inuse	None
7	smregion_0.smnode.appengine-7	pep	ums-0-1-smplaybackep-pep-ipvs-1	inuse	None
8	smregion_0.smnode.appengine-8	pep	ums-0-1-smplaybackep-pep-ipvs-0	inuse	None
9	smregion_0.smnode.mce-1	cep	ums-0-1-smcaptureep-cep-3	inuse	None

Backup/Restore User Interface

The following sections define the process to backup configuration from one PAM and restore to the other PAM.

1. Log in to PAM console, run “backup.py backup-dir” command.

```
i.e  “backup.py /root/backup-01”
backup-dir: it is a directory contains sub-directory/file
1: db sub-directiry:  mongo backup data.
```

```
2:  node.txt: node(s) information.
```

2. If reusing existing DNS, clean up is required. Assume that domain is “cisco.com” and ip address is “166.0.72.166”

- Run the following command to sync up.

```
rndc freeze cisco.com
rndc thaw cisco.com

rndc freeze 72.0.166.in-addr.arpa
rndc thaw 72.0.166.in-addr.arpa
```

- In /var/named/slaves, clean up db.cisco.com -
- remove entry containing “CNAME”
- remove entry containsing “pm-“ in prefix

```
i.e
pam-docserver CNAME   pm-35-1-8-106-VMP
pamds CNAME   pm-35-1-8-102-VMP
```

- remove entry that contains “se-“ in prefix

```
i.e
sr-11-0-0-83            A       11.0.0.83
ums          NS   sr-11-0-0-83
```

- In /var/named/slaves, clean up db.72.0.166
- Keep the following and remove everything else.

```
====================================
$ORIGIN .
$TTL 86400      ; 1 day
72.0.166.IN-ADDR.ARPA   IN SOA  dns.cisco.com. VMP.cisco.com. (
2012071023 ; serial
3600       ; refresh (1 hour)
1800       ; retry (30 minutes)
604800     ; expire (1 week)
86400      ; minimum (1 day)
)
NS      dns.cisco.com.
$ORIGIN 72.0.166.IN-ADDR.ARPA.
$TTL 30 ; 30 seconds
226                     PTR     dns.cisco.com.
============================================
```

3. Copy backup-dir to the new PAM.
4. Run “restore.py backup-dir” in the new PAM (just deployed from OVA).

Note: Do not run on a fully functional or failing PAM node.

```
backup-dir: backup directory in new PAM
This will also turn off all Life/VOD service.
```

5. Reboot the node. If the nodes are in an HA configuration, reboot each node in the cluster.
6. From GUI , turn the Life/VOD service(s) to active.
7. To exit the GUI at any time, click **Log out** at the top of any page.

Configuring the VMP Using the VMP Manager GUI

We recommend the following sequence of tasks when using the VMP Manager (VMP-M) GUI to configure the VMP.

- Logging into the VMP GUI, page 72
- Setting Up the VMP Infrastructure, page 50
- Creating Unified Media Services, page 50
- Creating Asset Workflows, page 52
- Asset File Download, page 59

For detailed information about the VMP Service Manager GUI, including descriptions of all of the fields on each page, see the VMP Service Manager GUI Reference, page 71.

Setting Up the VMP Infrastructure

The Infrastructure tab allows the user access to a list of pages for viewing and configuring various infrastructure components of VMP.

To configure each component, log in to the GUI as described in VMP Service Manager GUI Reference, page 71. Then, select the Infrastructure tab.

1. Configure **Software Image Manifests.** Refer to Configuring Software Image Manifests, page 91.
2. Configure **Regions & Zones.** Refer to Displaying and Configuring Regions and Zones, page 92.
3. Configure VMP **Nodes**. Refer to Configuring VMP Nodes, page 78.
4. Configure COS **Nodes.** Refer to Configuring COS Nodes, page 80.
5. Configure **COS Clusters.** Refer to Configuring COS Clusters, page 87.
6. Configure **COS Container Stores.** Refer to Configuring COS Container Stores, page 87.
7. Configure **NAS Stores.** Refer to .Configuring NAS Stores, page 89.

Creating Unified Media Services

Services define the MCE/MPE/AE nodes to be used for capture and playback.

The following are VMP requirements for the NFS server:

- We recommend that you use NFS version 4 with the VMP.
- The VMP must be able to write to the NFS server. Therefore, the NFS server must export a filer or directory with read/write access.
- For VOD service, the VMP requires write access to the NFS server that stores the indexed content.
- Disable the **async** export option in the NFS server configuration. That is, the NFS server is to reply to requests only after the changes have been committed to stable storage.

Use the following procedure to enable Media Service.

> **Note:** A minimum of 8 App Engines (2 Redis, 2 HA Proxy and 2 IPVS) are required to enable Media Service, otherwise service activation will fail.

1. To create a service, select **Services > Unified Media Service** to display the Service Summary page.

2. From the drop-down window, choose from the 3 available service types to create a new service for **LIVE, VOD** or **CDVR**.

The Service Domain objects available for the service chosen will appear at the top. Select and configure each object type to complete creating the service.

3. Choose an unused UMS Service and specify a name.

Note: The UMS Service instance includes a "Summary" which displays real time status of all associated capture/playback endpoints, nodes, and work flows.

4. Configure state cache endpoints for the service. State cache endpoints are used to cache content metadata used by the capture cluster. State cache endpoints are mandatory for enabling UMS for all services. Click **Save.**
   - Make sure the Name conforms to standard hostname specifications, as it is used by the APIs.
   - In the Desired Nodes field, enter the number of state cache endpoints that have been set up in the system. You can increase the number of desired nodes for SLA upgrade and decrease the number for SLA downgrade. This is supported for MCE, App Engine, and MPE.
   - Virtual IP (used by app engines for load balancing)
5. Configure capture endpoints for the service. Click **Save.**
   - Make sure the Name conforms to standard hostname specifications, as it is used by the APIs.
   - In the Desired Nodes field, enter the number of capture endpoints that have been set up in the system.
   - You can increase the number of desired nodes for SLA upgrade and decrease the number for SLA downgrade. This is supported for MCE, App Engine, and MPE.
   - Virtual IP (used by app engines for load balancing)
   - FQDN (defines the subdomain for capture urls) Example: mce.mos.npi.cds.cisco.com.
6. Configure playback endpoints for the service. Click **Save.**
   - Make sure the Name conforms to standard hostname specifications, as it is used by the APIs.
   - In the Desired Nodes field, enter the number of playback endpoints that have been set up in the system. You can increase the number of desired nodes for SLA upgrade and decrease the number for SLA downgrade. This is supported for MCE, App Engine, and MPE.
   - Virtual IP (used by app engines for load balancing)
   - FQDN (defines the subdomain for capture urls) Example: mce.mos.npi.cds.cisco.com.
7. Verify Capture/Playback endpoint configuration then set the Admin State to **Enable** and click **Save**.

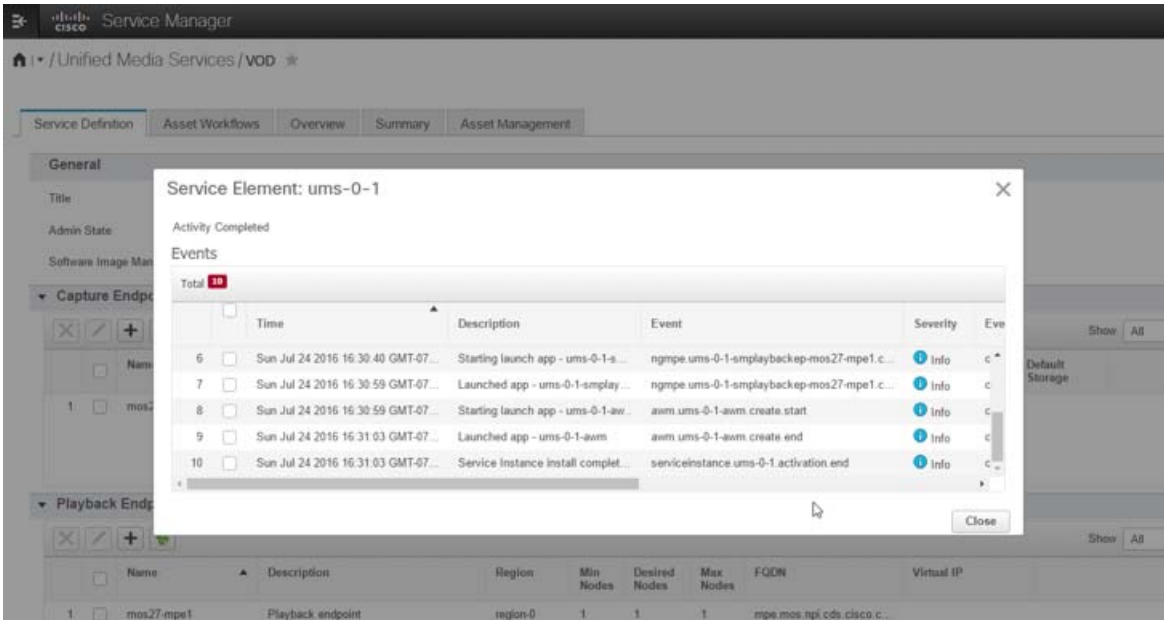
Enabling a service can take several minutes per node. For example, given a service with the following nodes:

- 4 MPE-Workers
- 4 MCE-Workers
- 8 App Engines
- 2 haproxy

- 2 MPE-ipvs
- 2 MCE-ipvs
- 2 state cache endpoints

It can take up to half an hour to enable the service. (10 nodes x 3 minutes per node = 30 minutes.) While a service is being enabled, the GUI ignores further attempts to perform actions or configuration tasks on that service.

VMP has an internal progress tracking feature to check the activity status. When a service is created/disabled, the progress tracking pop up window appears displaying all events associated with the service. VMP polls the events for approximately 15 seconds. If no events display, VMP stops polling. You can close the window at any time. To again see the progress activity, click the Activation status count bar at the top right corner of the page. When the status window shows Activity Complete, provisioning is done.



Note: The user should be able to activate/deactivate a service instance while the previous activate/deactivate service instance is not yet completed. Service instance activation/deactivation will take several minutes to complete. If the user tries to activate/deactivate while a previous activity is in progress, a popup message will appear alerting the user that a previous service activation is still in progress and if they want to deactivate the service.

Note: If the service activation/deactivation fails, the GUI will time out within 15 minutes.

8. To verify that all MPE/MCE/AE nodes have been successfully allocated to the service, select the **Overview** tab.

Creating Asset Workflows

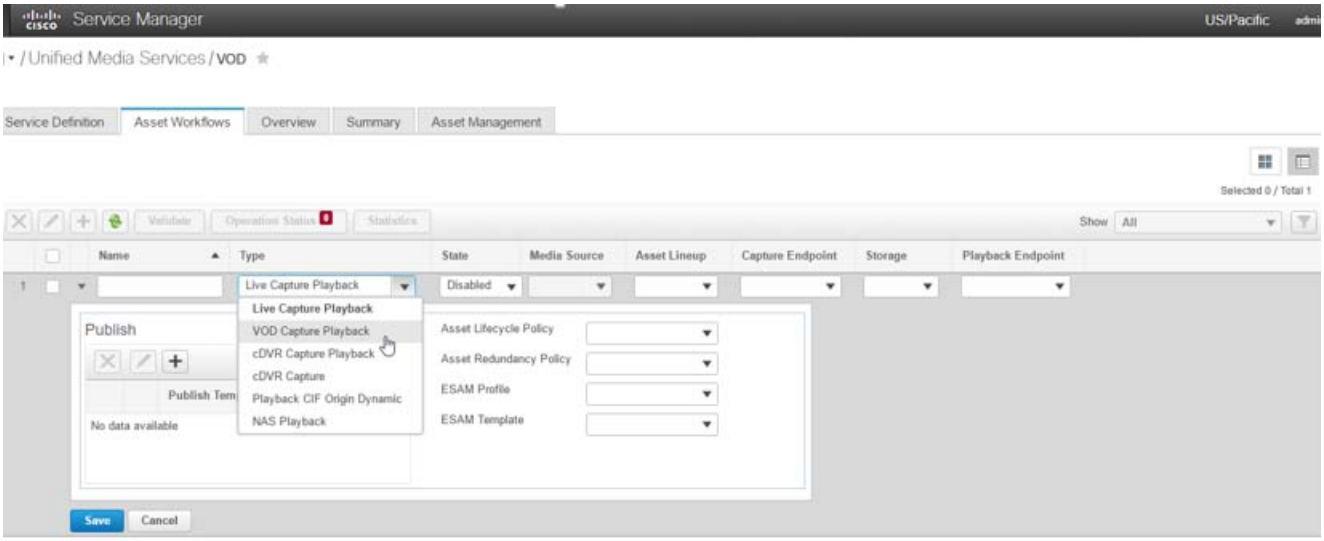
Once the Service Definition is enabled and assets provisioned, asset workflows can be created. Asset workflows define content source, how the content should be stored, secured and/or transformed and content delivery/publishing options.

the Workflows can be created in table or tile view. The Table view is used with the Legacy UI (2.2 version and older) and requires navigating to corresponding object pages to configure. The Tile view allows the user to set up assets all within the same view.

To create an Asset using the Table view, follow the steps below.

1. Select **Services > Unified Media Services.**
2. Click the **Asset Workflows** tab.

3. Select the Table view icon located in the upper right corner of the page.
4. Click the **+ button** then specify the name and type of workflow to create.
   - Live Capture Playback – This provides the user ability to configure an integrated capture and playback work flow for live assets.
   - VOD Capture Playback – This provides the user ability to configure an integrated capture and playback work flow for VOD assets
   - cDVRCapturePlayback – This provides the user ability to configure an integrated capture and playback work flow for cDVR assets.
   - cDVR Capture – This provides the user ability to configure a capture only work flow for cDVR assets.
   - Playback CIf Origin Dynamic – This provides the user the ability to configure a playback only work flow for cDVR assets, where the origin is discovered dynamically.
   - NasPlayback – This provides the user the ability to configure a playback work flow for assets stored in NAS.



5. Enable the asset work flow by changing the State field to **Enabled**, then click **Save**.

For a Live work flow, the asset is created as soon as the service and asset work flows are enabled, which can take up to several minutes.

For a VOD work flow, the service and asset work flow must first be enabled, then the asset must be created using the VMP Asset Management API.

For a NAS Playback work flow, the asset is created and stored directly in NAS by a third party. Once the work flow is enabled, the NAS will be mounted as a media source to MPE workers. The asset published URL looks like: http://<fqdn>/<awf name>-<publish template name>/<asset related path on NAS>.

Enabling an asset work flow can take up to several minutes per node. For example, given a work flow with the following nodes:

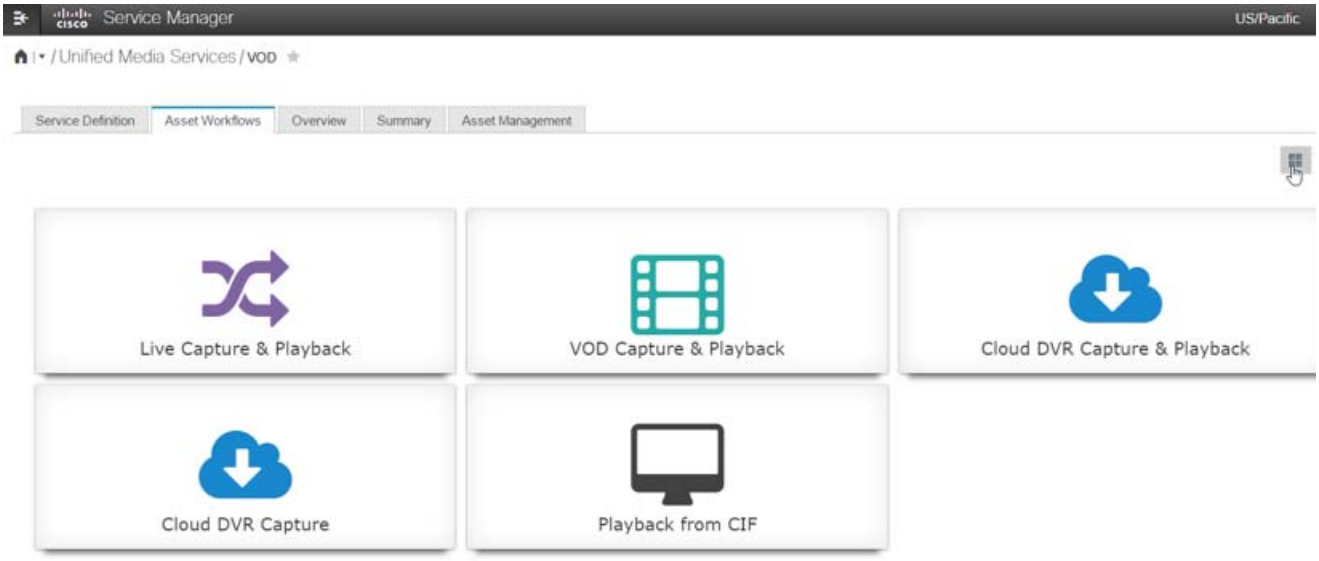
- 4 MPE-Workers
- 4 MCE-Workers
- 6 App Engines

It can take up to half an hour to enable the work flow. (10 nodes x 3 minutes per node = 30 minutes.) While a work flow is being enabled, the GUI ignores further attempts to perform actions or configuration tasks on that work flow.

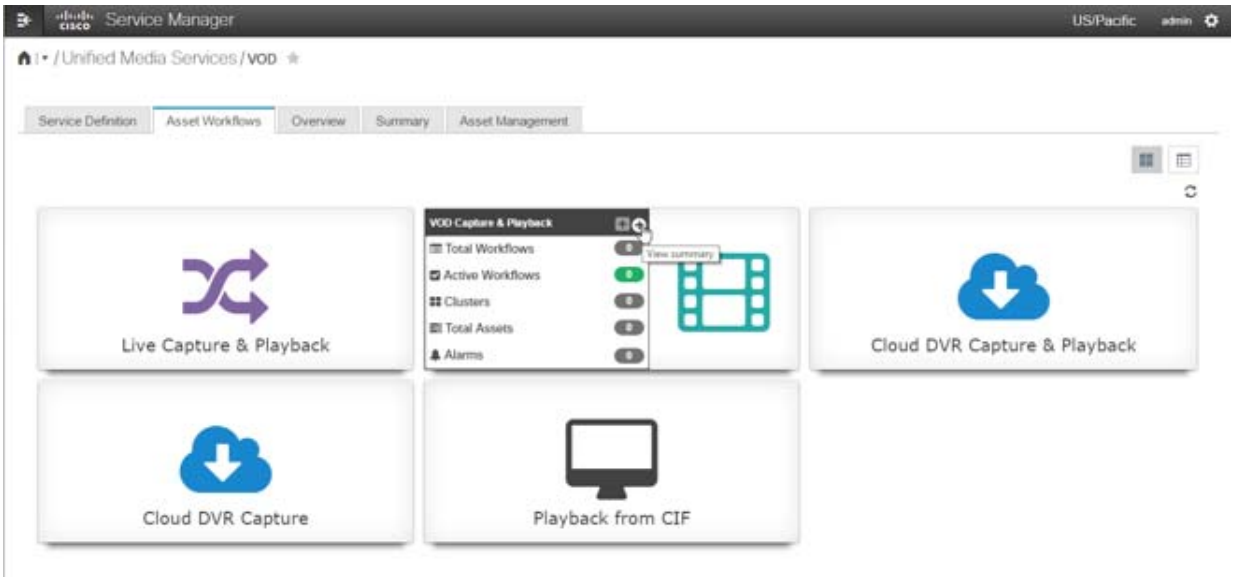
To determine whether a work flow has been enabled, VMP has an internal progress tracking feature. When a work flow is created/disabled, the progress tracking pop up window appears displaying all events associated with the work flow. VMP will poll the events for approximately 15 seconds. If no events display, VMP will stop polling. You can close the window at any time. To again see the activity, click the Activation status button.

To create an Asset using the Tile view, (updated menu experience) follow the steps below:

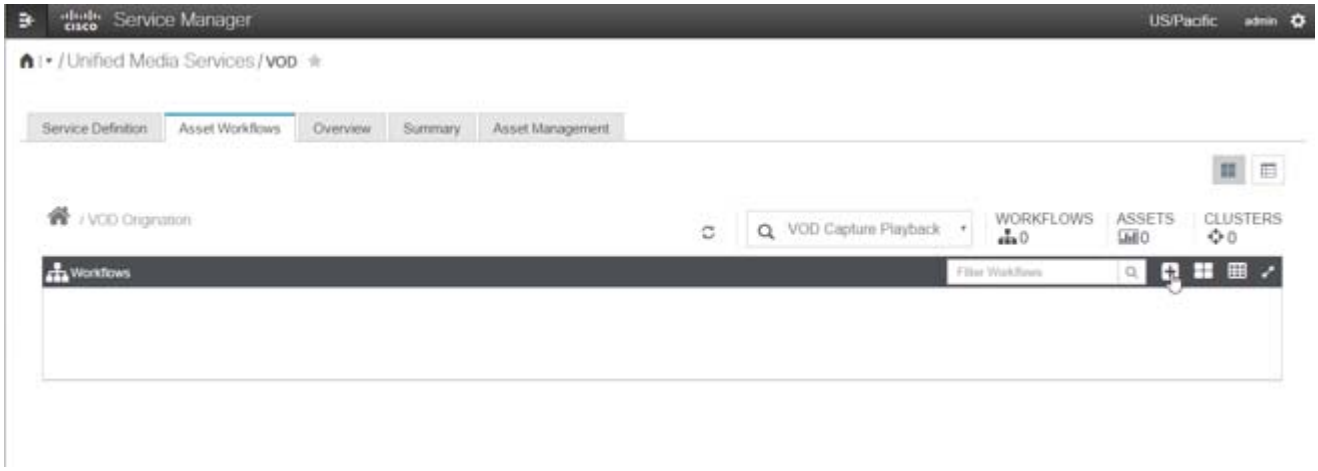
1. Click the Tile icon.
2. Select the workflow type from the available options:



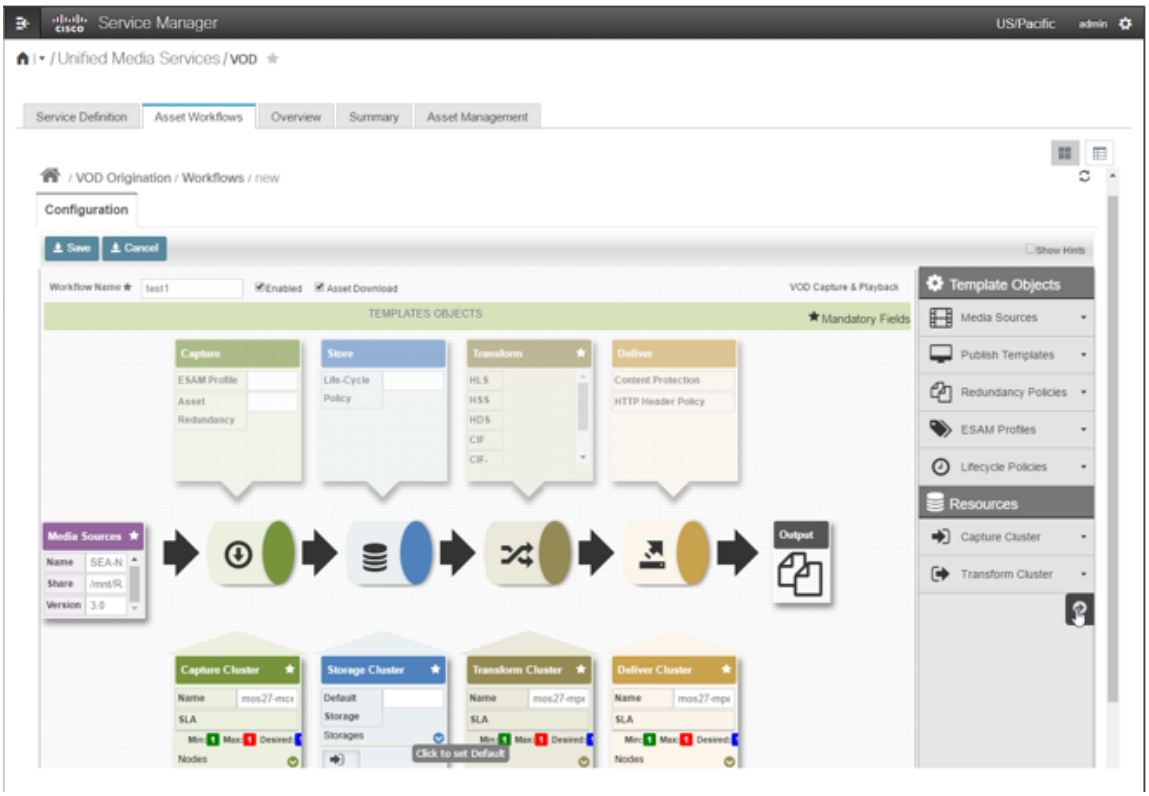
3. Click the view summary arrow icon to see all options for the workflow type selected.



4. Add a workflow.



5. The service Domain Objects will appear in the right tool bar. Expand the toolbar by selecting the arrow at the bottom.



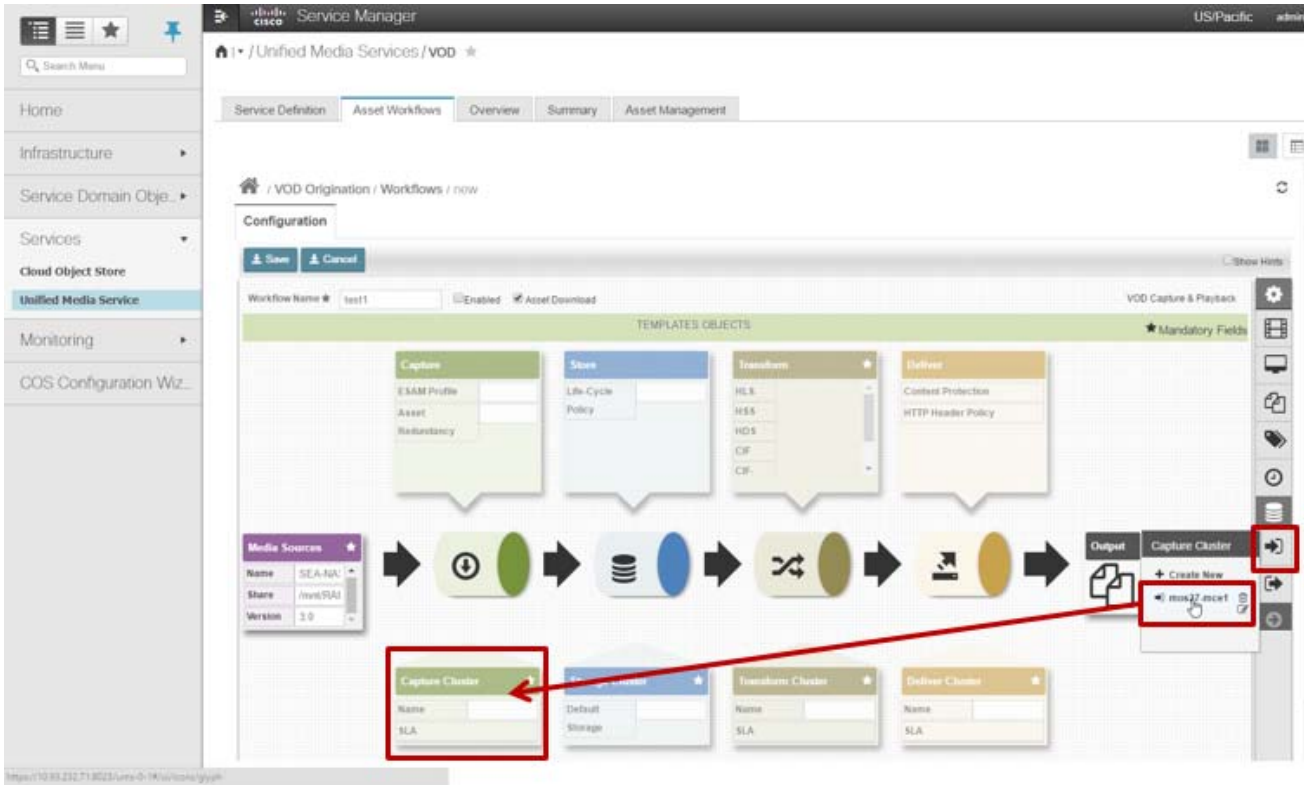
6. Objects already created may be selected. Select Media Sources> Create New tab for each object type not already defined.

7. Enter necessary details and click Save. The newly created media source will appear in the workflow.

8. Each field will need to be sequentially selected, working from left to right to complete the asset workflow.

9. Drag and drop each object from the right menu to its bucket on the left.

Note: If you need help with adding objects, click the “Show Hints” box at the top of the screen.



10. When all required template objects have been added, enter a name for your workflow and click **Enabled** and **Save**.

11. As objects are created in the Asset Workflow, they are added to the Service Domain Objects section of the navigation menu. Items created directly within the Service Domain Objects will appear in the Asset Workflow wizard for assignment.

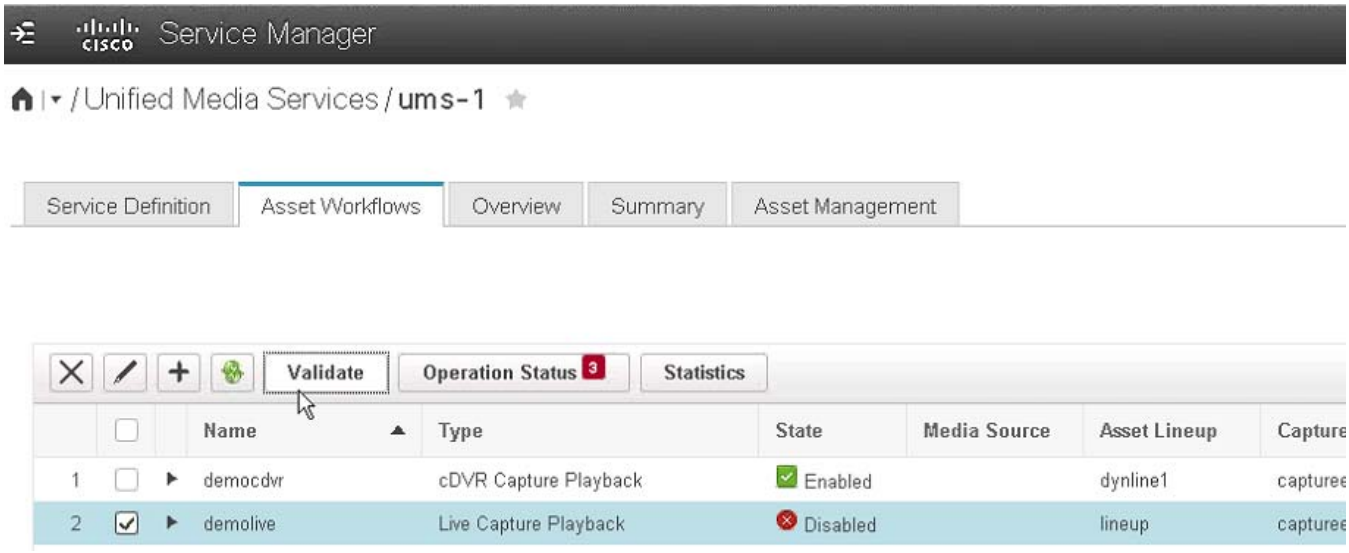
Asset Work Flow Validation

This feature allows the user to validate disabled work flows. Before enabling the service instance and work flow, resources associated with the work flow and service instance can be validated.

1. Select **Services > Unified Media Services-Asset Workflow**

2. Select the disabled work flow.

3. Click the **Validate** button.

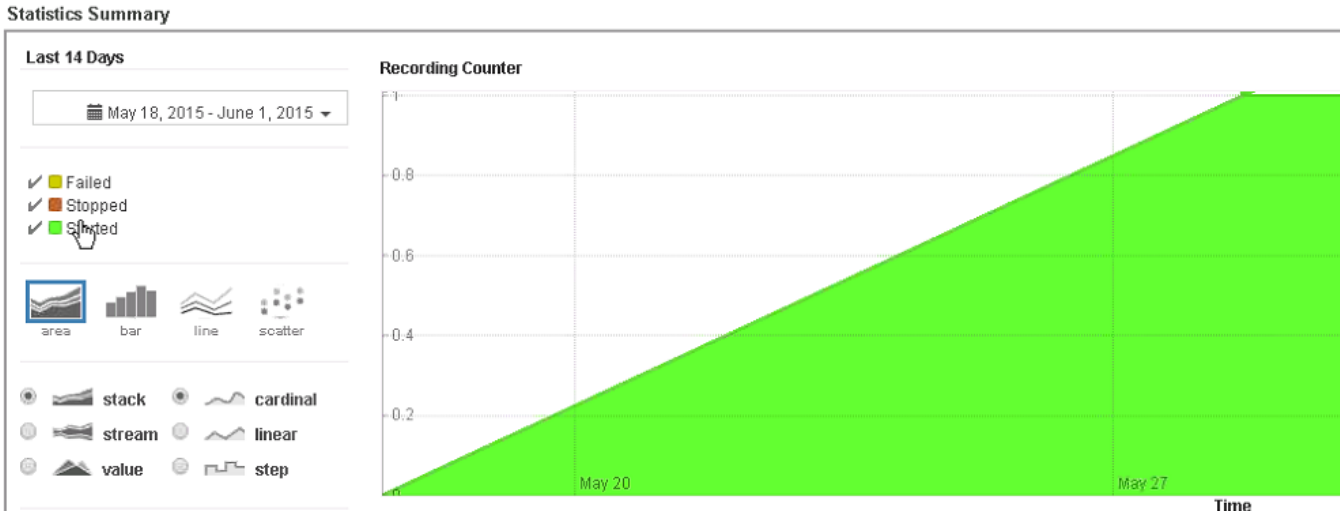


4. A polling pop-up window appears to show that VMP is validating the resources. The following resources will be validated:
   a. Capture endpoint SLA
   b. State cache endpoint
   c. Playback end point SLA
   d. Validate storage associated with the asset work flow
   e. Validate Media source associated with the asset work flow (VOD work flow)
   f. Validate if MCE node can receive configured channel, either UDP multi-cast feed or http feed
5. Click **Close** to close the window.

Asset Work Flow Management Statistics

This feature allows the user to check the state of each workflow asset. This feature can be used with the cDVR, Live, and VOD work flows.

1. Select the work flow, then click the **Statistics** tab.
2. A Statistics Summary chart will show data collected from the last 24 hours. If there is no data collected within the last 24 hours, the user can select a time frame from the drop-down window or enter a custom time period in the From/To boxes. Data will be shown in a graph indicating the number of resources in the Failed, Stopped, or Started state. The following graph display data collected for the last 14 days.



CDVR Scheduler

The VMP cDVR scheduler allows the user to schedule events for cDVR assets. When the first cDVR work flow is created, the AWM starts the scheduling process. Scheduling stops when there is no (enabled) cDVR work flow. The scheduler process is a timer loop which runs periodically in 30 second intervals.

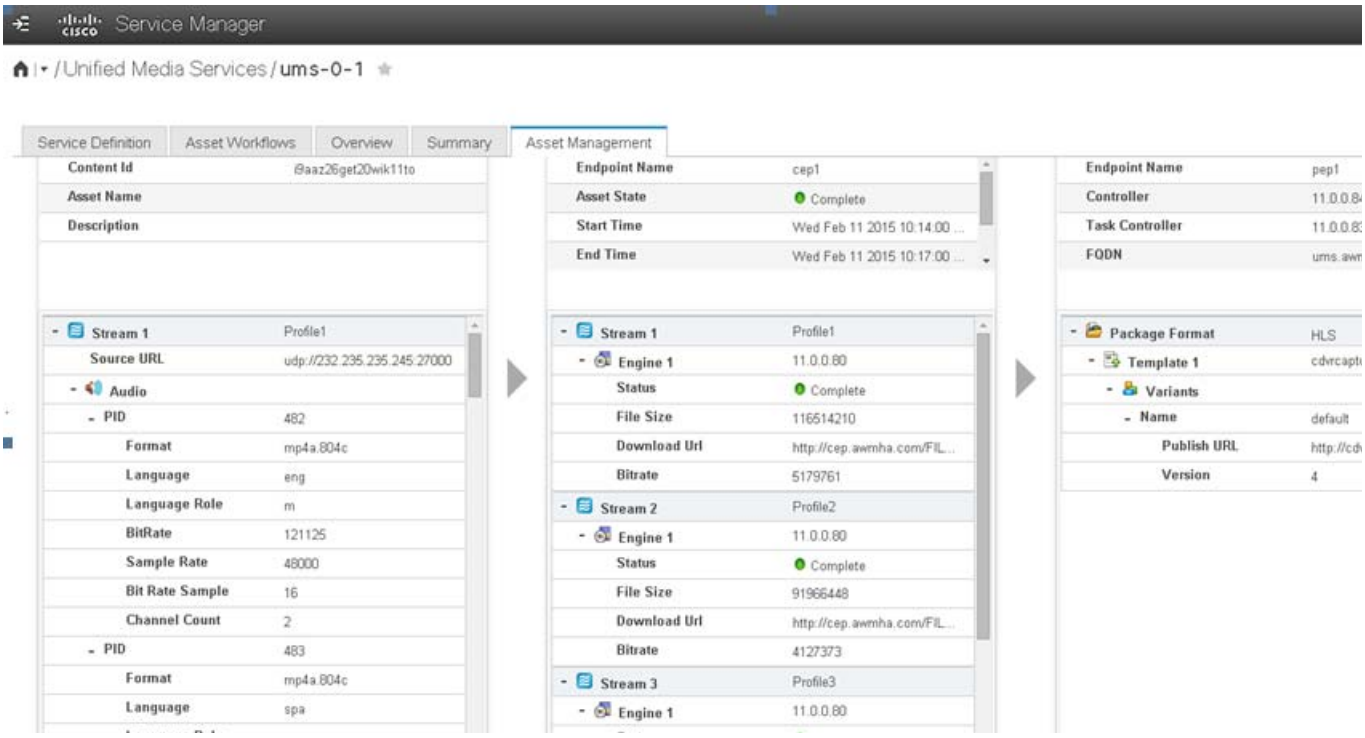
Asset File Download

The Asset file Download feature allows the user to download the source file of completed cDVR recordings. This feature is set by the user while configuring the cDVR work flow. After the cDVR recording is completed, the Asset Management page (see Asset Management tab in screen below) and the AWM API provides a url to download the source file from VMP.

1. Click the Asset Management tab.
2. In the work flow Select window, choose the work flow type.

Note: The “Asset Download” parameter and work flow must be set to **Enabled**.

3. Click **Apply.**
4. All assets for that work flow will be listed, including file size, download url, and bit rate.



Content Trimming

This feature provides support for users that want to download trimmed content from VMP.

To enable content trimming on VMP, follow the steps below.

1. Configure the channel with the stream type as " TS" for no-EBP content (50 Mbps/4:2:2 profile) instead of ATS.
2. Enable the live asset work flow with tstv/dvr window of 24hrs and set to capture mode.
3. Enable VOD asset work flow with asset download enabled.
4. Get the below resourceMpd url from the live asset status using AWM API
   a. " resourceMpd" :" http://100.7.43.161/live/4KCHAN/MPD?

5. Get the Capture start time and Capture end time from the progressiveDownload adaptation set from the live MPD file.
6. A content trim request can then be sent to VMP.
7. VMP Trims the VOD content with the Capture start and Capture end time using VOD ingest son file by POST method.
8. After ingest completes, a download url can be retrieved from the VOD asset status API.

COS Service for VMP

The Cisco Cloud Object Storage can be installed as a service of VMP. COS is designed to integrate transparently with VMP, and can be managed through the VMP GUI. COS provides distributed, resilient, high-performance storage and retrieval of binary large object (blob) data called objects. The primary interface for managing COS content is the OpenStack Swift API with enhancements that improve the quality of service when accessing large media objects. The Storage cluster is resilient against hard drive failure within a node and node failure within the cluster. Nodes may be added to or removed from the cluster as needed to provide for changes in the cluster's capacity. To administer the cluster, COS includes and HTTP-based cluster-management API. COS includes an HTTP-based cluster-management API. COS includes an authentication and authorization service that implements the OpenStack Swauth API. Object storage is distributed across a cluster of hardware systems, or nodes.

COS services are provided by software running on a set of nodes called a COS cluster that is connected by data and management networks.

Each COS cluster has a single fully-qualified domain name (FQDN) that is used by client applications to access COS services.

A COS cluster also has a number of configuration parameters that define the cluster's behavior.

Some of these parameters include the Swift and Swauth API constraints, the IP address pools used to assign IP addresses to individual node network adapters, and the IP address of the PAM configuration document server

To Configure COS for VMP, refer to Configuring COS Nodes, page 80.

Configuring COS Tunables

To prevent IOM timeout errors and to allow the MCE to conduct capture properly, the tcp keep alive COS tunables must be configured. This is set through an entry in a file on COS.

Filename/Path:

```
/arroyo/test/CalypsoTunables
```

File Entry:

```
tunables/tcp_timeout_ms 60000
```

Software Upgrade

This section outlines the procedure for upgrading an existing Centralized VMP Log Server (CLS) and PAM nodes.

We recommend upgrading the log server first. Make sure it is gathering information from all nodes, then upgrade PAM nodes. It could however be done in the reverse order.

CLS Upgrade

Currently, VMP supports a disruptive upgrade, meaning that during an upgrade, a cluster can be re-built but some log information on the centralized log server is missing (or stored locally). If this occurs, copy/save/backup the data from an old log server to the NAS or file server, then deploy and start a new log server.

In addition to sending log data to the CLS server, all processes save the log data locally. In the event of a network or service outage, check the local log files from the node under question first. Follow the steps below to perform the CLS upgrade.

1. Check functionality.
   a. Run **“service named status”** command to check if it is running on the DNS server.
   b. Each PAM node can resolve log server to the existing log server’s IP by running the command: **"nslookup log-server”**.
   c. Information (events and logs) on the log server is getting updated from all nodes.
2. Backup all data.
   a. FTP server with write permissions for user required.
   b. Before backing up data, stop logger server. Logging will be re-directed locally to each node.
   c. It is recommended that you rename the VM name to keep the old version running until a new node is fully functional. Once the CLS server is functional, it is safe to erase the old VM.
   d. Use the following script to backup data from the log server:

```
log_export FTP_SERVER_REMOTE_HOST USER_NAME PASSWORD
```

   e. Power off the logging server. If there are network disruptions or DNS server failures, logging will continue locally for each node. To recover all logging data during the upgrade, check all nodes, not just logging servers.
3. Deploy a new Version. Deploy a new logger node from the OVA and use the same parameters as in the older logger node and start the newly deployed node. We recommend using the same IP as an old server. As soon as the logger node starts, the A record will be pushed to the DNS server and all nodes will start sending data immediately.

2.33 Example:

```
/usr/bin/ovftool --name=log-server --datastore=datastore1 --powerOffTarget --overwrite --powerOn
--skipManifestCheck --acceptAllEulas --noSSLVerify --deploymentOption="VMP_LOG_SMALL_VM"
--prop:"hostname=log-server" --prop:"domain=testdns.com" --prop:"ip0=11.0.0.208"
--prop:"subnet0=255.255.255.0" --prop:"ntp0=11.0.0.111" --prop:"dns0=11.0.0.111"
--prop:"gateway0=11.0.0.1" --prop:"ext-dns-ip=11.0.0.111"
--prop:"ext-dns-key=ZSKgTDpuRAtG5E8M400BhA==" --prop:"ext-dns-algo=hmac-md5" --net:"Network for
adapter 1=Management" /home/abahel/stf_2/images/2.3.3-cisco-VMP-duncans.14905.ova
vi://root:cisco123@192.2.0.81/abahel-rack-z2-Blade-1/host/172.20.216.17
```

2.4 Example

```
/usr/bin/ovftool --name=log-server --datastore=datastore1 --powerOffTarget --overwrite --powerOn
--skipManifestCheck --acceptAllEulas --noSSLVerify --deploymentOption="VMP_LOG_SMALL_VM"
--prop:"hostname=log-server" --prop:"domain=testdns.com" --prop:"ip0=11.0.0.208"
```

```
--prop:"subnet0=255.255.255.0" --prop:"ntp0=11.0.0.111" --prop:"dns0=11.0.0.111"
--prop:"gateway0=11.0.0.1" --prop:"ext-dns-ip=11.0.0.111"
--prop:"ext-dns-key=ZSKgTDpuRAtG5E8M400BhA==" --prop:"ext-dns-algo=hmac-md5" --net:"Network for
adapter 1=Management" /home/abahel/stf_2/images/2.4.0-cisco-VMP-mendocino.15023.ova
vi://root:cisco123@192.2.0.81/abahel-rack-z2-Blade-1/host/172.20.216.17
```

4. Check that all data is coming from all nodes by using the UI console.

PAM Upgrade

1. Disable all work flows. (Wait until all workflows are disabled).

Go to the following link, and make sure all workflows are disabled:

```
https://service-mgr:8443/#pageId=com_cisco_VMP_page_services_ums
```

2. Disable all services. (Wait until all services are disabled).

Go to the following link and make sure all services are disabled:

```
https://service-mgr:8443/#pageId=com_cisco_VMP_page_services_ums
```

3. Backup all existing VMP PAM nodes.

We suggest running back up commands for all PAM nodes (it will save unique state.json and nodes info). Replace the word “node” with actual data for the PAM node (domain name or IP) and replace “user/your_server” with the credentials of the place where you want to store the back up files:

```
ssh admin@node
sudo /opt/cisco/VMP/bin/backup.py backup
tar czf backup.tar.gz backup
scp backup.tar.gz user@your_server:backup-VMP.tar.gz
```

Example:

```
Nodes are 11.0.0.211, 11.0.0.212, 11.0.0.213, mongo leader is 11.0.0.211
ssh admin@11.0.0.211 "sudo /opt/cisco/VMP/bin/backup.py backup;tar czf backup.tar.gz backup"
scp admin@11.0.0.211:backup.tar.gz backup-VMP.tar.gz
ssh admin@11.0.0.212 "sudo /opt/cisco/VMP/bin/backup.py backup;tar czf backup.tar.gz backup"
scp admin@11.0.0.212:backup.tar.gz backup-VMP.tar.gz
ssh admin@11.0.0.213 "sudo /opt/cisco/VMP/bin/backup.py backup;tar czf backup.tar.gz backup"
scp admin@11.0.0.213:backup.tar.gz backup-VMP.tar.gz
```

4. Power off all 3 PAM nodes.

Note: It's a good idea to rename VM names and keep them until the entire procedure is complete and confirmed.

5. Deploy a new VMP cluster. Using the VMPt recent OVA image and parameters (same as in the old VM OVA properties for each node), deploy all new nodes.

Example:

```
Rename ab-pam-01 -> ab-pam-01old, ab-pam-02 -> ab-pam-02old, ab-pam-03 -> ab-pam-03old.
ovftool --noSSLVerify --acceptAllEulas --powerOffSource --overwrite --powerOn --diskMode=thin
--prop:"ext-dns-ip=11.0.0.111" --prop:"ext-dns-key=ZSKgTDpuRAtG5E8M400BhA=="
--prop:"ext-dns-algo=hmac-md5"  --prop:"peer0=11.0.0.212"  --prop:"peer1=11.0.0.213"
--prop:"ip0=11.0.0.211" --net:"Network for adapter 1=Management" --prop:"ntp2=64.104.193.12"
--prop:"dns2=11.0.0.111" --name="ab-pam-01" --datastore="datastore1" --prop:"ntp0=11.0.0.111"
--prop:"dns0=11.0.0.111" --prop:"admin-password=default" --prop:"ntp1=10.81.254.202"
--prop:"domain=testdns.com" --prop:"subnet0=255.255.255.0" --prop:"gateway0=11.0.0.1"
--prop:"dns1=11.0.0.111" --prop:"hostname.cisco=ab-pam-01"
images/2.4.0-cisco-VMP-mendocino.15023.ova
vi://root:cisco123@192.2.0.81/abahel-rack-z2-Blade-1/host/172.20.216.17/
```

```
ovftool --noSSLVerify --acceptAllEulas --powerOffSource --overwrite --powerOn --diskMode=thin
--prop:"ext-dns-ip=11.0.0.111" --prop:"ext-dns-key=ZSKgTDpuRAtG5E8M400BhA=="
--prop:"ext-dns-algo=hmac-md5"  --prop:"peer0=11.0.0.211"  --prop:"peer1=11.0.0.212"
--prop:"ip0=11.0.0.213" --net:"Network for adapter 1=Management" --prop:"ntp2=64.104.193.12"
--prop:"dns2=11.0.0.111" --name="ab-pam-03" --datastore="datastore1" --prop:"ntp0=11.0.0.111"
--prop:"dns0=11.0.0.111" --prop:"admin-password=default" --prop:"ntp1=10.81.254.202"
--prop:"domain=testdns.com" --prop:"subnet0=255.255.255.0" --prop:"gateway0=11.0.0.1"
--prop:"dns1=11.0.0.111" --prop:"hostname.cisco=ab-pam-02"
images/2.4.0-cisco-VMP-mendocino.15023.ova
vi://root:cisco123@192.2.0.81/abahel-rack-z2-Blade-1/host/172.20.216.17/
ovftool --noSSLVerify --acceptAllEulas --powerOffSource --overwrite --powerOn --diskMode=thin
--prop:"ext-dns-ip=11.0.0.111" --prop:"ext-dns-key=ZSKgTDpuRAtG5E8M400BhA=="
--prop:"ext-dns-algo=hmac-md5"  --prop:"peer0=11.0.0.211"  --prop:"peer1=11.0.0.213"
--prop:"ip0=11.0.0.212" --net:"Network for adapter 1=Management" --prop:"ntp2=64.104.193.12"
--prop:"dns2=11.0.0.111" --name="ab-pam-02" --datastore="datastore1" --prop:"ntp0=11.0.0.111"
--prop:"dns0=11.0.0.111" --prop:"admin-password=default" --prop:"ntp1=10.81.254.202"
--prop:"domain=testdns.com" --prop:"subnet0=255.255.255.0" --prop:"gateway0=11.0.0.1"
--prop:"dns1=11.0.0.111" --prop:"hostname.cisco=ab-pam-03"
images/2.4.0-cisco-VMP-mendocino.15023.ova
vi://root:cisco123@192.2.0.81/abahel-rack-z2-Blade-1/host/172.20.216.17/
```

6. Check a new VMP cluster and establish a leader.

   a. When reusing existing IP and DNS parameters, some clean up might be required. Refer to Backup/Restore User Interface, page 48, step 2.

   b. Check all 3 PAM nodes. tail -f /var/log/opt/cisco/VMP/error/* should not show any recurring errors. If errors occur, refer to Troubleshooting the PAM, page 136 or repeat steps starting from step 5.

   c. Check to make sure the GUI is operational. If errors occur, refer to Troubleshooting the VMP-M GUI, page 121.

7. Restore previous configuration.

   a. For the leader node, run the following command, replacing “nodeIP” with actual data for the node (domain name or IP):

```
scp backup-VMP.tar.gz admin@nodeIP:backup.tar.gz
ssh admin@nodeIP
tar xvf backup.tar.gz
sudo /opt/cisco/VMP/bin/restore.py backup
sudo /opt/cisco/VMP/bin/nodeRestore.py backup"
```

   b. Restart all nodes.

Example:

```
scp backup-VMP.tar.gz admin@11.0.0.211:backup.tar.gz
ssh admin@11.0.0.211 "tar xvf backup.tar.gz;sudo /opt/cisco/VMP/bin/restore.py backup;sudo
/opt/cisco/VMP
/bin/nodeRestore.py backup"
```

8. Check the GUI to make sure you can see all Nodes and all services. If some are missing, refer to Troubleshooting the VMP-M GUI, page 121 or repeat steps 7 onward.

9. Start all services. Go to the following link, and enable all needed services (sometimes it might take up to 5 mins per service, but wait until operation completes:

```
https://service-mgr:8443/#pageId=com_cisco_VMP_page_services_ums
```

10. Start all work flows and check streaming. Go to following link, and make sure all proper work flows are enabled:

```
https://service-mgr:8443/#pageId=com_cisco_VMP_page_services_ums
```

11. Check the browser for streaming.

The VMP PAM cluster should be functional.

Upgrading the MCE or AppEngine OVAs

For this operation to work without causing the service to fail, additional node capacity above the current SLA minimum is required. The additional nodes must be in idle state prior to upgrading other nodes. Upgrading while a service is active may affect end user services, therefore it is recommended that all asset workflows and/or services are disabled before upgrading the nodes.

To upgrade a node:

1. Go to Infrastructure > Compute> Nodes and set the node to Maintenance Admin state.
2. Refresh the screen to make sure that it goes to maintenance operation state and that it is not in alarm.
3. Ensure that one of the additional MCE or AppEngine nodes that was in idle state has replaced the one in maintenance state.
4. Deploy the new OVA for that particular node either manually or using the VMware ovftool command. Perform any necessary post-deployment operations, such as configuring additional interfaces, static routes or additional commands. If possible, watch the VCenter console to ensure the node comes up correctly.
5. When the node is up, return to the node list and ensure there are no alarms shown for that node. Return the node from Admin state back to Inservice and ensure that it goes to idle state.
6. Repeat this process for each node you plan to upgrade.
7. Enable any asset workflows and/or services disabled and make sure that all nodes are used as necessary to meet SLA requirements.

RPM-Based Upgrade

This document outlines the manual steps necessary to do an RPM upgrade of an App-Group. App-Groups can be upgraded on either a SuperOVA-based or a RPM-based VM. The upgrade process only upgrades an App-Group to the latest version of RPMs contained in the Repository VM.

The devices should be upgraded in the following order when the system is in Service:

MPE > MCE> AE > Log Server> PAM1 > PAM 2 > PAM 3

Software Images Required

VMP minimal bootstrap RPM:

```
/auto/VMP2/cdvrbld/published_area/release_builds/2.4.1-cisco-VMP-mendocino.2.4.1-latest/cisco-VMP-minimal-bootstrap-2.4.1-<buildNo>.x86_64.rpm
```

Upgrade Procedure

Follow the steps below to perform the RPM upgrade.

1. Setup and login to the Repository VM for your test-bed, and mount the **new** MOS ISO containing the new version of MOS software (to be upgraded to) as follows:

```
umount /var/www/html/mos/repo/2.8
mount <path/to/new/MOS/ISO> /var/www/html/mos/repo/2.8
```

```
systemctl restart httpd
```

2. Login to the MOS Service Manager GUI and disable the UMS.
3. Move all MCE/MPE/Appengine nodes to maintenance mode.
4. Install **mosUpgrade** on all nodes, for example:

```
rpm -ivh
http://192.168.106.176/mos/repo/2.8.xxx/yumrepo/cisco-mos-minimal-bootstrap-2.8.xxx-21156.x86_64.rpm
```

5. Run the **mosUpgrade** utility on all nodes (to be upgraded) and start upgrade procedure

Note: The following can run simultaneously to reduce upgrade time.

```
mce
/opt/cisco/mos/upgrade/bin/mosUpgrade --repourl http://192.168.106.176/mos/repo/2.8.xxx --appname
mce-app --shutdown
mpe
/opt/cisco/mos/upgrade/bin/mosUpgrade --repourl http://192.168.106.176/mos/repo/2.8.xxx --appname
mpe-app --shutdown
appengine
/opt/cisco/mos/upgrade/bin/mosUpgrade --repourl http://192.168.106.176/mos/repo/2.8.xxx --appname
appengine --shutdown
logger
/opt/cisco/mos/upgrade/bin/mosUpgrade --repourl http://192.168.106.176/mos/repo/2.8.xxx --appname
logger-app --shutdown --nomaintenance
pam
/opt/cisco/mos/upgrade/bin/mosUpgrade --repourl http://192.168.106.176/mos/repo/2.8.xxx --appname
pam-app --shutdown --nomaintenance
```

6. After upgrading all nodes including the PAM, change the image type to MPE, and image version to the latest.
7. Update image manifest version to the latest.
8. Move all nodes from Maintenance Mode to “In Service Now”.
9. Enable UMS.

Limitations

For PAM VM upgrades, limited regression testing has currently been performed.

(Basic PAM upgrade functionality has been verified.)

OpenStack

OpenStack’s technology consists of a series of interrelated projects which controls a given deployment of hardware providing processing, storage, and networking. Deployments are managed using a simple UI and flexible API which can be used by third party software. As a standard RPM based software application, VMP can easily run as a virtual machine. To run VMP on OpenStack, 4 logical networks are required:

- Management Network
- Video Data In Network (live feed, VOD content repo, storage (COS/NAS)).
- Video Data Out Network (CDN facing, or client facing)
- Data Internal Network

There are 3 network topologies:

1. All-in-one:
   - all 4 logical networks are in one physical network
2. On-premise (recommended)
   - Management Network
   - Video Data In Netoerk
   - Video Data Out and Data Internal Network are in one physical network
3. Public cloud – each logical network maps to one physical network (recommended)

Deploying VMP on OpenStack

Once the OpenStack environment is up and running, you can deploy the VMP clusters and configure the VMP cluster to do Live and VOD services.

Minimum Required OpenStack Version

- Openstack Juno – 2014.2.4
- Openstack Kilo – 2015.2.4
- Openstack Liberty

OpenStack Topology

Controller + (N) Compute nodes with Provider networking

(N) – 1 or more compute nodes

Minimum Required Services on OpenStack

- Identity (Keystone)
- Image (Glance)
- Compute (Nova)
- Networking (Neutron)
- Dashboard (Horizon)
- Orchestration (Heat)

VMP Cluster Deployment

The user can perform two types of VMP cluster OpenStack deployments – RPM and SuperOVA. See instructions below.

RPM-Based Deployment

1. Configure DNS Server.
2. Configure REPO VM.
3. Deploy VMP Cluster using Heat Template for RPM Based Deployment.

4. The following images should be used:
   a. 2.7.0-cisco-VMP-centos7-mendocino.<LATEST VERSION>.ova – base image
   b. 2.7.0-cisco-VMP-mendocino.<VERSION>.iso – To be used to configure REPO
   c. cisco-VMP-minimal-bootstrap-<VERSION>.x86_64.rpm – To be used to configure REPO
   d. cisco-VMP-repo-bootstrap-<VERSION>.x86_64.rpm – To be used to configure REPO
5. The following templates should be used (based on network topology)
   a. VMP_cluster_rpm_1_network.yml
   b. VMP_cluster_rpm_2_network.yml
   c. VMP_cluster_rpm_3_network.yml
   d. VMP_cluster_rpm_4_network.yml

SuperOva-Based Deployment

1. Configure DNS Server
2. Deploy VMP Cluster using Heat Template for SuperOVA based deployment
3. The following image should be used:
   a. 2.7.0-cisco-VMP-mendocino.<VERSION>.ova
4. The following templates should be used (based on network topology):
   a. VMP_cluster_superova_1_network.yml
   b. VMP_cluster_superova_2_network.yml
   c. VMP_cluster_superova_3_network.yml
   d. VMP_cluster_superova_4_network.yml

Template Parameters

The user has to provide real values for the template parameters based on the OpenStack setup when the template is deployed. The following examples provide template parameters with sample values.

admin_password:

default: default

description: Admin Password

hidden: true

label: Admin Password

type: string

cep_vip:

default: 172.20.203.76

description: VIP address for Capture End Point

label: Virtual IP for CEP

type: string

data1_network_id:

default: 219a5a32-0e6c-4903-bc5e-f11f440cfb53

description: Network ID to be used as Data1 Network

label: Data1 Network ID

type: string

data2_network_id:

default: b3b13017-241b-4456-af9a-7e87e5f4956b

description: Network ID to be used as Data2 network

label: Data2 Network ID

type: string

data3_network_id:

default: b3b13017-251b-5456-af9a-7e87e5f4956b

description: Network ID to be used as Data3 network

label: Data3 Network ID

type: string

domain_name:

default: VMP.com

description: Domain Name

label: Domain name

type: string

ext_dns_algo:

default: hmac-md5

description: External DNS Algorithm (Example, HMAC-MD5)

label: External DNS Algorithm

type: string

ext_dns_ip:

default: 172.20.203.70

description: External DNS IP Address

label: External DNS IP

type: string

ext_dns_key:

default: ujLdXfCZenQZQKZlFy42fw==

description: External DNS Key

label: External DNS Key

type: string

flavor_name:

default: m1.medium

description: Name Flavor to use for server

label: Flavor Name

type: string

image_name:

default: Centos7-15604

description: Name of the image to use for PAM, MCE, APP-ENGINE, LOG-SERVER, MPE

(rpm based) nodes

label: Image Name for PAM, MCE, APP-ENGINE, LOG-SERVER, MPE (rpm based)

type: string

logserver_device_mode:

constraints:

- allowed_values:

- VMP_LOG_SMALL_VM

- VMP_LOG_MEDIUM_VM

- VMP_LOG_LARGE_VM

description: Device mode value must be VMP_LOG_SMALL_VM or VMP_LOG_MEDIUM_VM or VMP_LOG_LARGE_VM for LOG-SERVER

default: VMP_LOG_MEDIUM_VM

description: Device Mode for LOG-SERVER

label: Device Mode for LOG-SERVER

type: string

management_network_id:

default: 80a43c40-9940-466d-b276-4ee59e7a0332

description: Network ID to be used as Management Network

label: Management Network ID

type: string

ntp_ip:

default: 10.81.254.202

description: NTP IP Address

label: NTP IP

type: string

pep_vip:

default: 172.20.203.77

description: VIP address for Playback End Point

label: Virtual IP for PEP

type: string

radius_ip:

default: None

description: Radius IP Address

label: Radius IP

type: string

radius_secret:

default: None

description: Radius Secret

label: Radius Secret

type: string

scep_vip:

default: 172.20.203.75

description: VIP address for State Cache End Point

label: Virtual IP for SCEP

type: string

VMP Service Manager GUI Reference

The VMP Gui enables you to quickly and easily access many VMP deployment and monitoring functions.

Before you Begin

When working with the VMP Service Manager GUI, keep the following considerations in mind:

- The VMP Service Manager GUI can run on the following operating systems and browsers:
  - Windows Internet Explorer 9 (IE9) or later for Windows 7
  - Mozilla Firefox 20 or later for Windows 7
  - Google Chrome 30.x for Windows 7
  - Apple Safari 7.x for Windows 7 or MAC OS Version 10.9 or later
- The VMP Service Manager GUI requires a display resolution of 1600 x 900 or better.
- If the PAM IP Address on which you are accessing the VMP Service Manager GUI is NATed, response time can be noticeably slow.
- The GUI times out after one hour (60 minutes) of inactivity. To avoid timeouts, make and save a configuration change, or click a tab or refresh icon, before the one-hour idle timeout expires.
- Configuration changes that you make in any section of the GUI are saved when you click the **Save** button. If you log out of the GUI, or if the GUI times out, before you save your changes, all changes that you have made since your last save are lost.
- If you try to delete an object in the GUI that has been associated with another object (for example, a capture endpoint that has been associated with an asset work flow), the GUI prevents the deletion and displays an explanatory error message.
- If you redeploy or upgrade the VMP OVA, you must clear your browser cache for the VMP Service Manager GUI changes to take effect.

This section provides the following information:

- Logging into the VMP GUI, page 72
- Working with the VMP Service Manager GUI, page 73
- Working with Pages in the VMP Service Manager GUI, page 75
- Displaying High-Level Overview Information for the VMP, page 76
- Configuring VMP Nodes, page 78
- Configuring COS Nodes, page 80
- Configuring COS Clusters, page 87
- Configuring COS Container Stores, page 87

- Configuring COS Node Initialization Profiles, page 88
- Configuring File System Gateway (FSG) Tenant, page 88
- .Configuring NAS Stores, page 89
- Editing Platform Services, page 89
- Configuring Software Image Manifests, page 91
- Displaying and Configuring Regions and Zones, page 92
- Configuring Channels, page 93
- Configuring NAS Media Sources, page 95
- Configuring Channel Lineups, page 95
- Configuring ESAM Profiles, page 100
- Configuring HTTP Header Policies, page 103
- Configuring Asset Lifecycle Policies, page 104
- Configuring Asset Redundancy Policies, page 105
- Configuring Subtitle Policies, page 107
- Configuring Publish Templates, page 108
- Configuring ESAM Templates, page 110
- Configuring an Asset Workflow, page 112
- Displaying System Diagnostics, page 112
- Displaying Service Diagnostics, page 114
- Displaying Logs, page 116
- Analyzing Logs, page 117
- Displaying Events, page 118

Logging into the VMP GUI

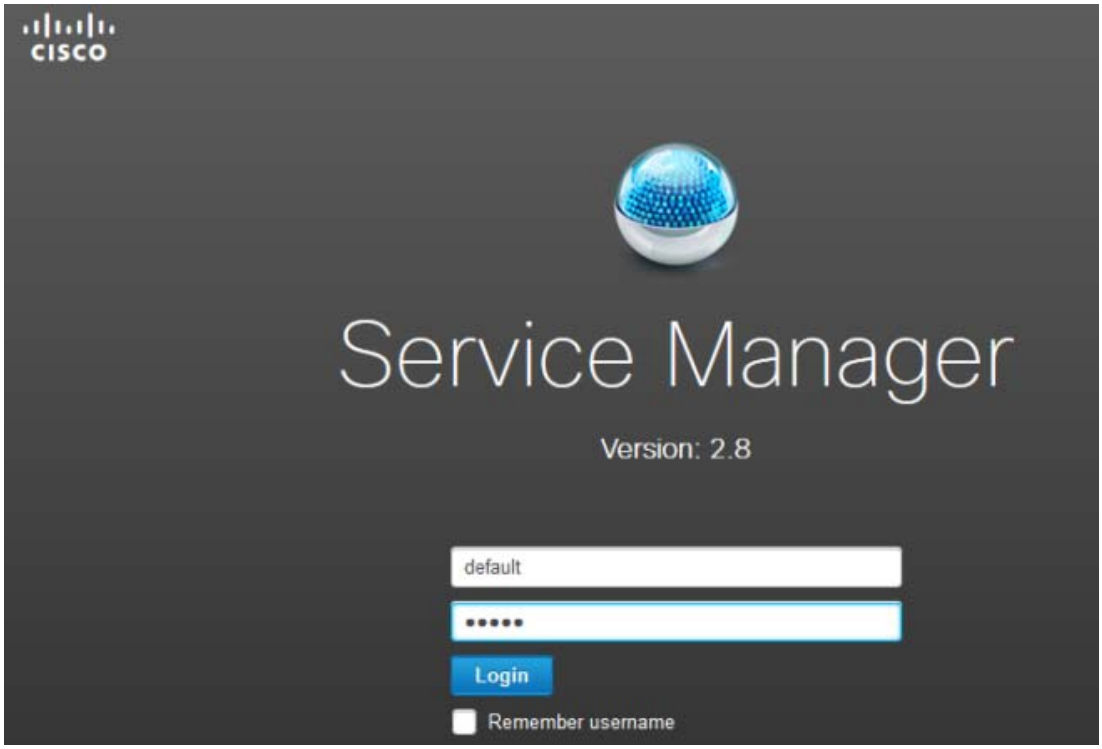
To log in to the VMP GUI, use the following procedure:

1. Access the GUI using the PAM IP Address. The URL format is

https://*pam_dns_entry***:8443**

2. Log in to the GUI with your Username and Password.

The default username is **admin**. The default password for local authentication is **default**. We recommend that you change these after deployment is complete.



3. The main page of the GUI is displayed. Select a tab at the top of the page to begin working with the GUI.
4. To exit the GUI at any time, click **Logout** at the top of any page.

Working with the VMP Service Manager GUI

Usernames and Passwords

After deployment, the VMP stores the GUI username and password on the PAM VM in the /etc/opt/cisco/VMP/public. Authentication is done using REST APIs.

We recommend that you change the default username and password after installation.

Time Zone

To set the time zone to use for VMP Service Manager GUI timestamps, select **admin > Preferences**. For more information, see the Setting the Time Zone for Timestamps, page 76.

Home

To display high-level overview information for the VMP, select **Home**. For more information, see the Displaying High-Level Overview Information for the VMP, page 76.

Infrastructure

To configure VMP infrastructure, select **Infrastructure**, then select a configuration option.

To work with	Select	For more information
Nodes	**Compute > Nodes**	Configuring VMP Nodes, page 78
COS Nodes	Storage > COS Nodes	Configuring COS Nodes, page 80

To work with	Select	For more information
COS Node Clusters	Storage > COS Node Clusters	Configuring COS Clusters, page 87
COS Container Stores	Storage > COS Container Stores	Configuring COS Container Stores, page 87
COS Node Initialization Profiles	Storage > COS Node Initialization Profiles	Configuring COS Node Initialization Profiles, page 88
File System Gateway	Storage > File System Gateway (FSG) Tenant	Configuring File System Gateway (FSG) Tenant, page 88
Network Attached Storage (NAS) stores	**Storage > NAS Stores**	.Configuring NAS Stores, page 89
Dynamic Lineup	**Asset Lineup > Dynamic Lineup**	Configuring Dynamic Lineups, page 98
Platform services, including NTP servers, DNS servers, and DNS forwarders	**Platform Services**	Editing Platform Services, page 89
Software Image Manifests	**Software Image Manifests**	Configuring Software Image Manifests, page 91
Regions and Zones	**Regions & Zones**	Displaying and Configuring Regions and Zones, page 92

VMP Service Domain Objects

To configure VMP service domain objects, select **Service Domain Objects**, then select a configuration option.

Table 0-1

To work with	Select	For more information
Channels	**Media Sources > Channels**	Configuring Channels, page 93
NAS media sources	**Media Sources > NAS Media Sources**	Configuring NAS Media Sources, page 95
Dynamic Sources	Media Sources > Dynamic Sources	Configuring Dynamic Sources, page 95
Channel lineups	**Asset Lineups > Channel Lineups**	Configuring Channel Lineups, page 95
Dynamic Lineup	**Asset Lineups > Dynamic Lineups**	Configuring Dynamic Lineups, page 98
Auth profiles	**Profiles > Auth Profiles**	Configuring Auth Profiles, page 99
ESAM profiles	**Profiles > ESAM Profiles**	Configuring ESAM Profiles, page 100
Key profiles	**Profiles > Key Profiles**	Configuring Key Profiles, page 101
HTTP header policies	**Policies > HTTP Header Policies**	Configuring HTTP Header Policies, page 103
Asset Lifecycle policies	**Policies > Asset Lifecycle Policies**	Configuring Asset Lifecycle Policies, page 104
Asset Redundancy policies	**Policies > Asset Redundancy Policies**	Configuring Asset Redundancy Policies, page 105
Subtitle Policies	**Policies > Subtitle Policies**	Configuring Subtitle Policies, page 107
Publish Templates	**Templates > Publish Templates**	Configuring Subtitle Policies, page 107
ESAM Templates	**Templates > ESAM Templates**	Configuring ESAM Templates, page 110

Monitoring the VMP

To monitor the VMP, select the **Monitor** tab, then select a monitoring option.

Table 0-2

To work with	Select	For more information
System diagnostics	**Diagnostic Settings > System Diagnostics**	Displaying System Diagnostics, page 112
Service diagnostics	**Diagnostic Settings > Service Diagnostics**	Displaying Service Diagnostics, page 114
Logs	**Logs > Log Viewer**	Displaying Logs, page 116
Log analysis	**Logs > Log Analysis**	Analyzing Logs, page 117
Events	**Events**	Displaying Events, page 118

Working with Pages in the VMP Service Manager GUI

Most of the tables displayed in the VMP Service Manager GUI enable you to add, edit, and delete entries; sort entries by column; change the order of columns; and use filters to control what is displayed.

Add an Entry

To add an entry to a table, click **the + button** at the top of the table. Enter or select values for the new entry, then click **Save** to add it to the table or select **Cancel** to Cancel the selection.

Edit an Entry

Use the expand/collapse button to **Edit** an entry. The row becomes read only and the Edit icon is active. Click the **edit (pencil icon)** to edit your entry

Select an Entry

Single click the row.

Delete an Entry

To delete an entry from a table, select the entry and click **the X button** at the top of the table. When prompted, click **OK**. The entry is removed from the table.

Refresh a Table

To refresh the entries in a table, click the **Refresh** icon at the top of the table.

Sort Entries

To sort entries in a table based on the contents of a column, click the column header. Click once to order the table in alphanumeric ascending order; click twice for descending order.

Change Order of Columns

To change the order of columns in a table, drag-and-drop the column headings.

Filter Contents

To filter the contents of a table, select a filter in the drop-down box at the top-right of the table, or click the **Filter** icon to toggle between the different filters.

- **All**—Display all of the table contents. This is the default display.
- **Quick Filter**—Display only those elements of one or more columns that contain specified text strings.
- **Advanced Filter**—Display only those elements of the table that match a set of one or more rules that you specify.

  For each rule, specify a column; a type of filter, such as **Contains** or **Starts with**; and a text string.

  To add another rule to the filter, click the plus sign (**+**). You can specify more than one rule for a given column.

If you have specified more than one rule, the **Match** drop-down box is displayed.

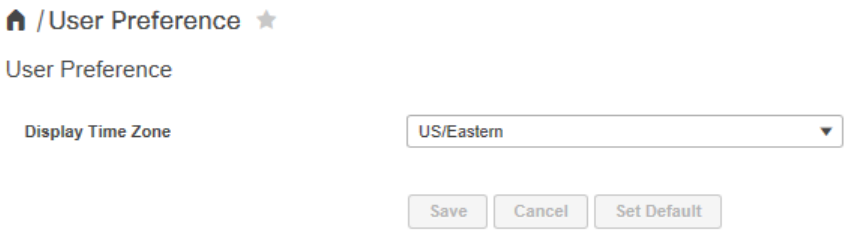
- To specify that an element of the table must match all of the specified rules in order to be included in the list, select **Match > All**.
- To specify that an element of the table need only match one or more of the specified rules in order to be included in the list, select **Match > Any**.
- To delete a rule from the filter, click the minus sign (**-**).
- To apply the filter to the elements of the table, click **Go**.
- To clear the filter and display all elements of the table, click **Clear Filter**.

- **Manage Preset Filters**—Edit or remove Advanced Filters that you have saved.

Note: When you refresh the page in your browser, all saved filters are removed.

Setting the Time Zone for Timestamps

To set the time zone to use for VMP Service Manager GUI timestamps, select **admin > Preferences** in the VMP Service Manager GUI. The User Preference page displays the Time Zone drop-down box.



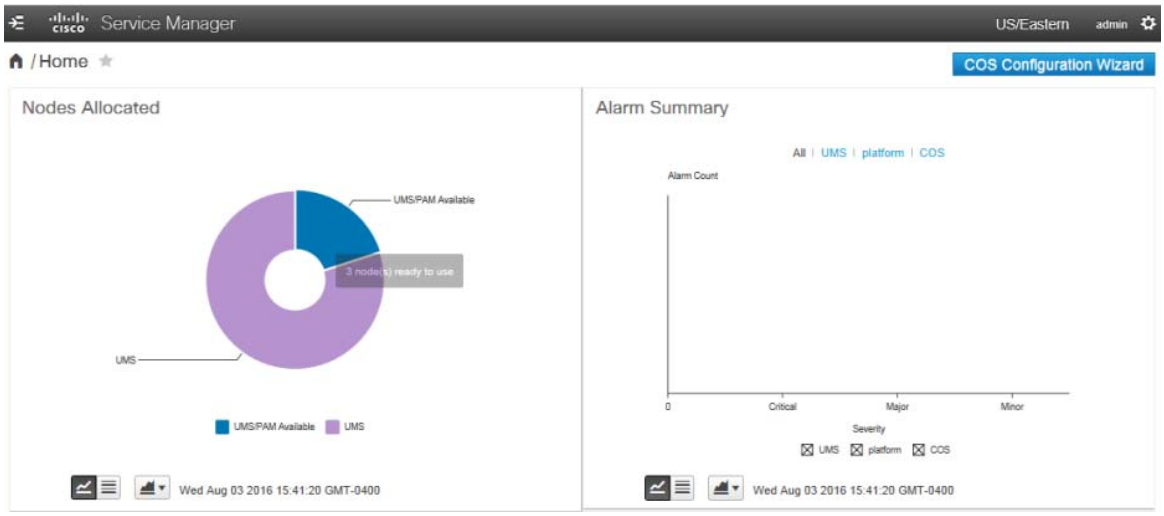
Select your time zone from the Time Zone drop-down box.

Update Default System CLI Login

To update a default user name and cli password, select **admin > Preferences** in the VMP Service Manager GUI. The User Preference page displays the Default drop-down box.

Displaying High-Level Overview Information for the VMP

To display high-level overview information for the VMP, select **Home** in the VMP Service Manager GUI. The Home page displays the following information for the VMP, automatically refreshed every five (5) minutes.



Nodes Allocated

The Nodes Allocated section of the Home page displays the allocation of VMP nodes, broken down by service type (such as Live or VOD), available nodes, and nodes that are in maintenance mode. You can display node allocation in pie chart or tabular format.

Alarm Summary

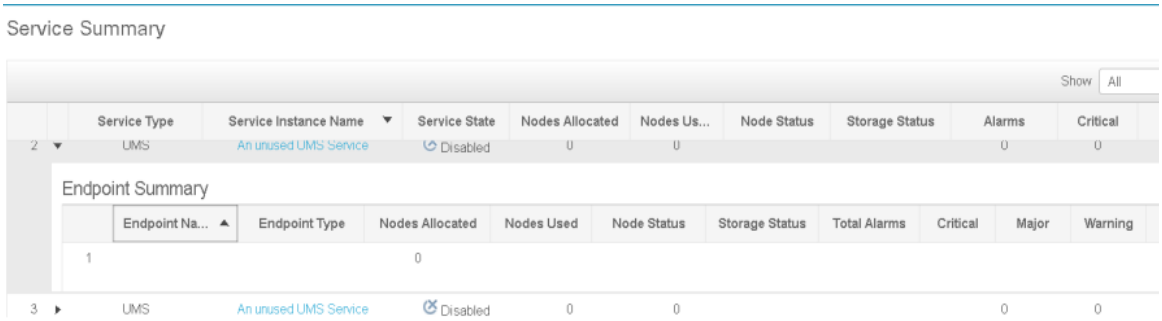
The Alarms Count by Service Type section of the Home page displays the number of alarms logged for each service type, further broken down by severity of the alarms (critical, major, or minor). You can toggle among several types of charts or tabular format.

Service Summary

The Service Summary section of the Home page displays the following information for each VMP node (you cannot edit these fields):

- Service Type—Type of service instance, such as **UMS** or **COS**.
- Service Instance Name—Name of the service instance.
- Service State—Indicates whether the service instance is currently **Enabled** or **Disabled**.
- Nodes Allocated—Number of nodes allocated for use by the service instance.
- Nodes Used—Number of nodes currently being used by the service instance.
- AppStatus—Current status of the node associated with the service instance.
- Storage Status—Current status of the storage associated with the service instance.
- Total Alarms—Total number of alarms logged for the service instance.
- Critical—Number of Critical alarms logged for the service instance.
- Major—Number of Major alarms logged for the service instance.
- Warning—Number of Warning alarms logged for the service instance.

To display the endpoint summary for a service instance, click its **Expand** arrow.



The Endpoint Summary table displays the following information for each endpoint (you cannot edit these fields):

- Endpoint Name—Name of the endpoint.
- Endpoint Type—Type of endpoint. Valid values are **Capture** and **Playback**.
- Nodes Allocated—Number of nodes allocated for use by the endpoint.
- Nodes Used—Number of nodes currently being used by the endpoint.
- Nodes Status—Current status of the node associated with the endpoint.
- Storage Status—Current status of the storage associated with the service instance.
- Total Alarms—Total number of alarms logged for the service instance.
- Critical—Number of Critical alarms logged for the service instance.
- Major—Number of Major alarms logged for the service instance.
- Warning—Number of Warning alarms logged for the service instance.

To collapse the interface information, click the **Collapse** arrow.

Configuring VMP Nodes

Note: Before adding any nodes, verify that there is connectivity between the PAM and the nodes' management IP address.

All MCE, App Engine, and MPE nodes in a region that use the same Image Type, Image Version, and Personality must have identical route configurations.

1. To add, edit, or delete nodes, select **Infrastructure > Compute > Nodes** in the VMP Service Manager GUI.
2. Click the **+** sign to add a node.
3. Enter the node details and click **Save**.

The GUI automatically refreshes the Nodes table every 60 seconds.

The Nodes table displays the following information for each node:

- Name—Name of the node (required). The name is a string of up to 63 characters. Acceptable characters include uppercase and lowercase letters and hyphens (-). The name must begin with a letter, and it is not case-sensitive.
- Description—Description of the node. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
- Zone—Zone with which the node is associated.

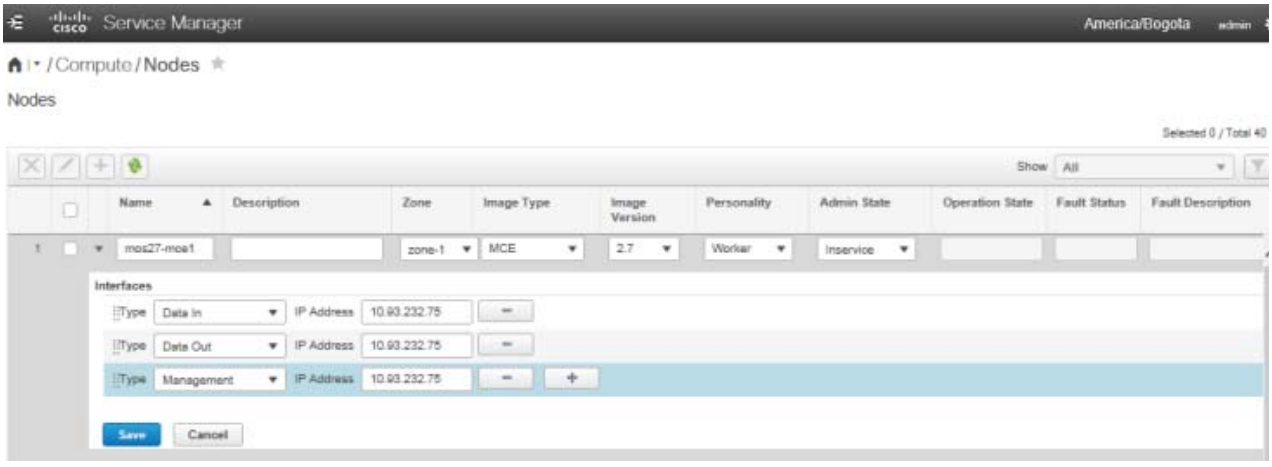
- Image Type—Image associated with the node. Valid values are **MCE, App Engine, MPE** and **NG-MPE**.
- Image Version—Description of the version of the image associated with the node. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.

  Note: The image version for a node must match the version configured in the associated software image manifest. For more information, see the Configuring Software Image Manifests, page 91.
- Personality—Personality of the image associated with the node.
  - For Image Tag **MCE**, the only valid value is **Worker**.
  - For Image Tag **MPE**, the only valid value is **Worker**.
  - For Image Tag **App Engine,** the only valid value is **Worker**.
- Admin State—Administrative status of the node. Valid values are **Inservice** and **Maintenance**.
- Operation State—Operational status of the node. You cannot edit this field. Valid values are **In-Use**, **Idle**, **Maintenance**, and **Pending**.
- Fault Status—Fault state of the node. You cannot edit this field. Valid states are:
  - **None**—No current fault.
  - **Warning**—Minor fault, node can still be used.
  - **Critical**—Major fault, node cannot be used.
- Fault Description—Description of the fault. You cannot edit this field.

When you first create a node, the Operation State, Fault Status, and Fault Description fields are empty. The GUI automatically populates these fields when you refresh the page by pressing **F5** or clicking the **Refresh** icon.

The following screen example is for the MCE. At least 6 App engine nodes,1 MCE and 1 MPE node must be added for a minimal deployment.

To display/configure the interfaces associated with a node, click its **Expand** arrow. For lab deployments with 1 network design, the Data In/Out/management Interfaces need to be designated and 1 IP Address identified.



- The Interfaces table displays the following information for each interface:

  - Type—Type of interface.

    - For MCE-Worker, valid values are **Data In**, **Data Out**, and **Management**.

    - For MPE-Worker, valid values are **Data In**, **Data Out**, and **Management**.

  - IP Address—IP address of the interface.

- To add, delete, or edit the interfaces for a node, select the node and click **Edit** at the top of the table.
  - Click the plus sign (**+**) to add an interface.
  - Click the minus sign (**-**) to delete an interface.
  - Enter or select new values for any interfaces that you want to edit.
- Click the **Collapse** arrow to collapse the interface information.

If you want to delete or modify a node in the GUI, and the node is **Inservice**, use the following procedure:

1. Select the node, click **Edit**, set the Admin State to **Maintenance**, and click **Save**.
2. Shut down the actual node, to prevent the VMP from connecting to it. (If the node is a VM, you can use vCenter to shut it down.)
3. When the VMP determines that it can no longer connect to the node (after approximately five minutes), the GUI sets the Operation State of the node to **Maintenance**.
4. Select **Infrastructure > Compute > Nodes** and verify that the Operation State of the node is set to **Maintenance**.
5. You can now delete or modify the node.

- To delete the node, select it and click **Delete**. The node is removed from the Nodes table.
- To modify the node, select it and click **Edit**. Make your changes to the node's configuration, then set the Admin State to **Inservice** and click **Save**.

6. Power on the node. When the VMP connects to the node (after approximately five minutes), the GUI sets the Operation State of the node to either **In-Use** or **Idle**, depending on whether the VMP is using the node at the time.

Application Instance Controller (AIC)

Follow the steps below to enable/disable AIC. The default status is disabled

1. Navigate to the User Preference Page.
2. For the Node Allocation Policy, select IPVS Assignment.
3. Click **Save**. The "Node Allocation saved successfully" message appears.
4. AIC is now enabled. Navigate to the "Nodes" page to verify.

To disable the AIC, follow the steps above. In step number 2, select "Default Assignment". AIC is now disabled.

Configuring COS Nodes

In COS version 3.8.1, the Configuration Wizard can be created through the user interface so that individual COS Node configuration of the following files is not required:

/arroyo/test/setupfile

/arroyo/test/SubnetTable

/arroyo/test/RemoteServers

/etc/cassandra/conf/cassandra.yaml

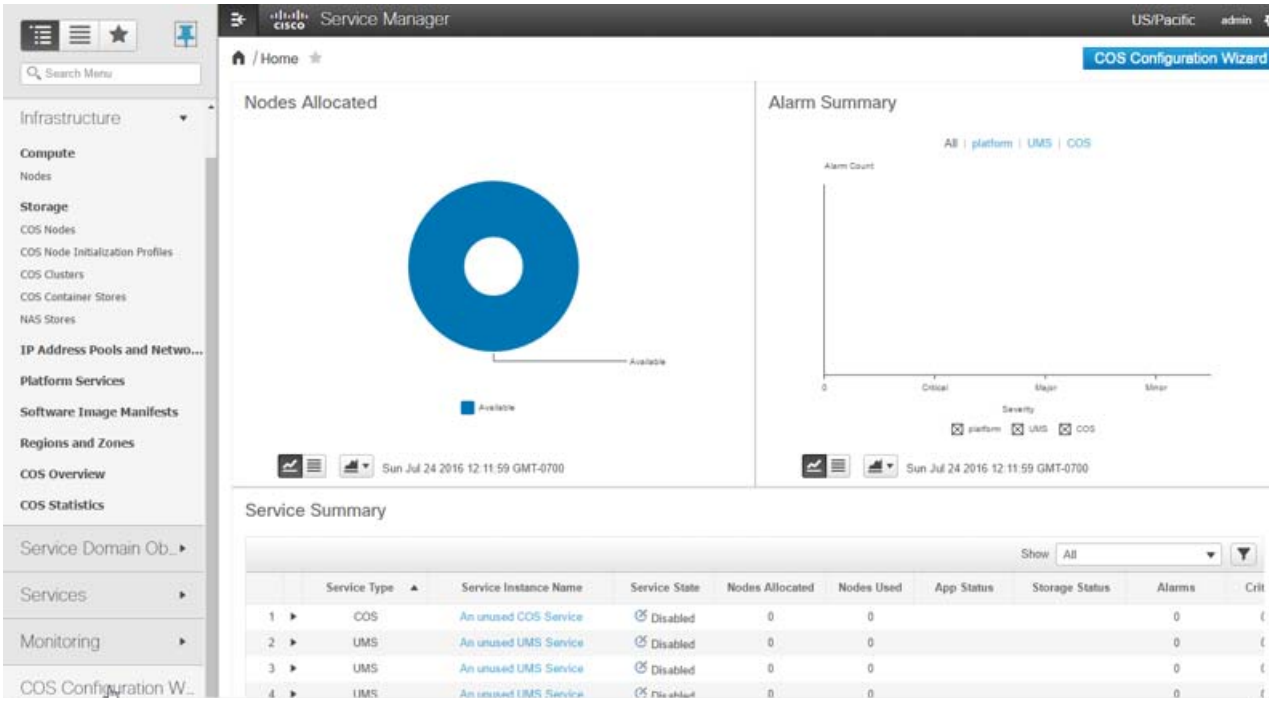
/etc/cosd.conf

/opt/cisco/cos/config/cos.cql

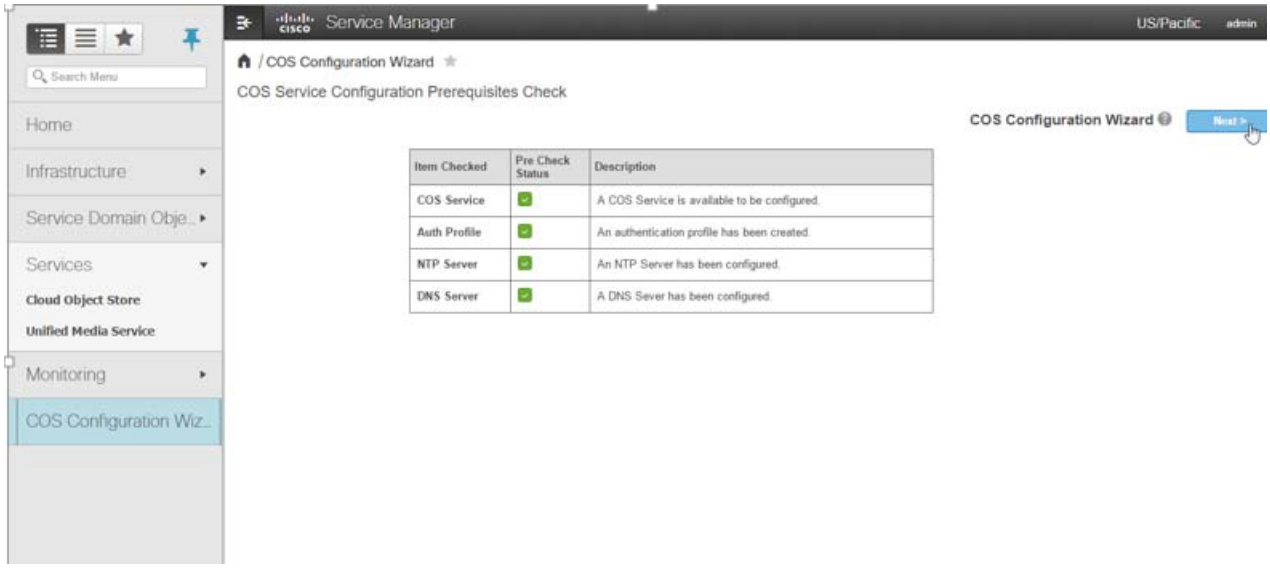
It also guides the user through the required UI configuration steps. The Configuration Wizard is available on the Home Screen and in the Navigation window. The wizard allows sequential creation of the COS configuration items required.

To configure COS nodes, follow the steps below.

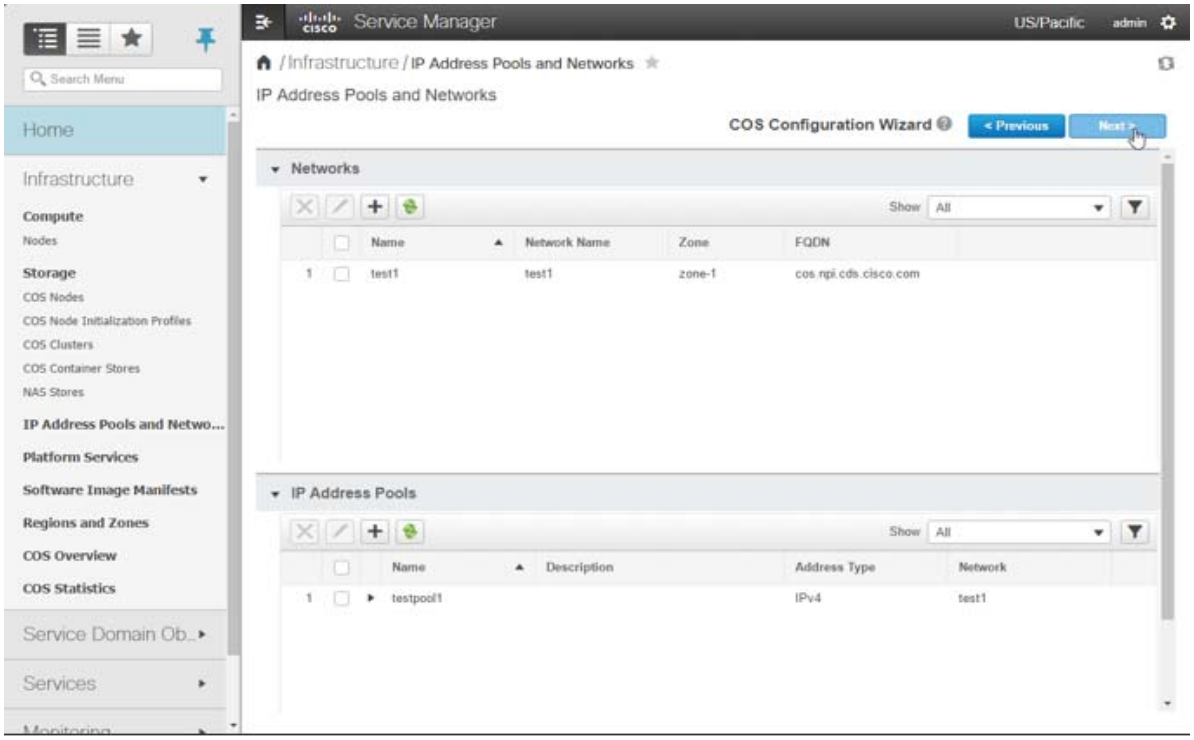
1. Select the COS Configuration tab on the home screen or in the navigation window.



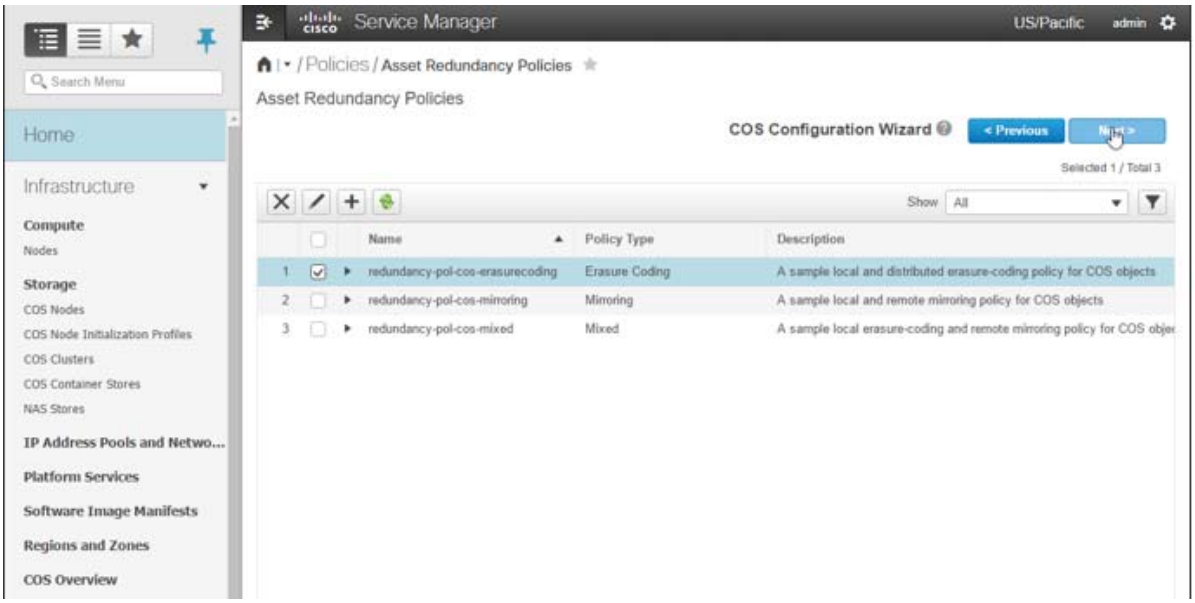
2. The Prerequisites window appears verifying that all is in place.



3. Click **Next.** The wizard will allow sequential creation of the COS configuration items required. See Below
   - COS Nodes
   - COS Node Initialization Profiles
   - COS Clusters
   - COS Container Stores
   - NAS Stores
   - IP Address Pools and Networks
4. Add Networks and IP Address Pools, then click **Next**.

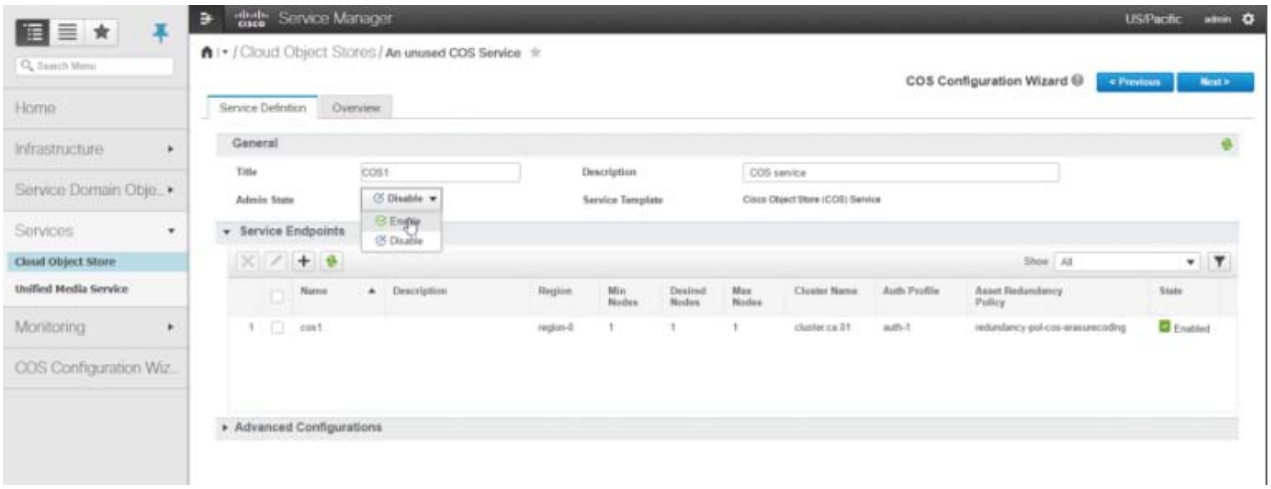


5. Select an Asset Redundancy Policy, then click **Next.**

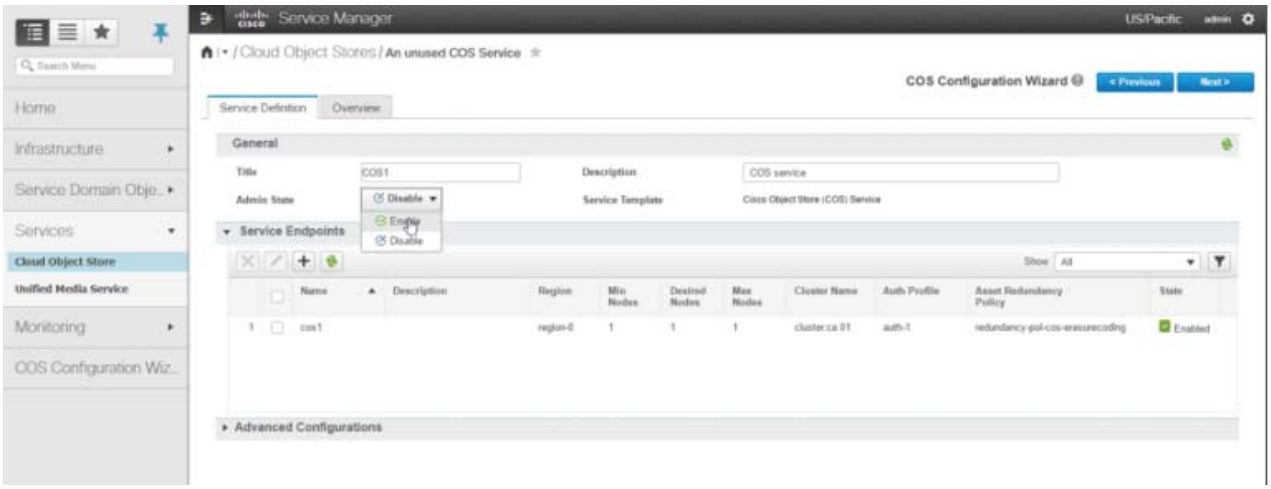


6. Create a cluster, then click **Next.**

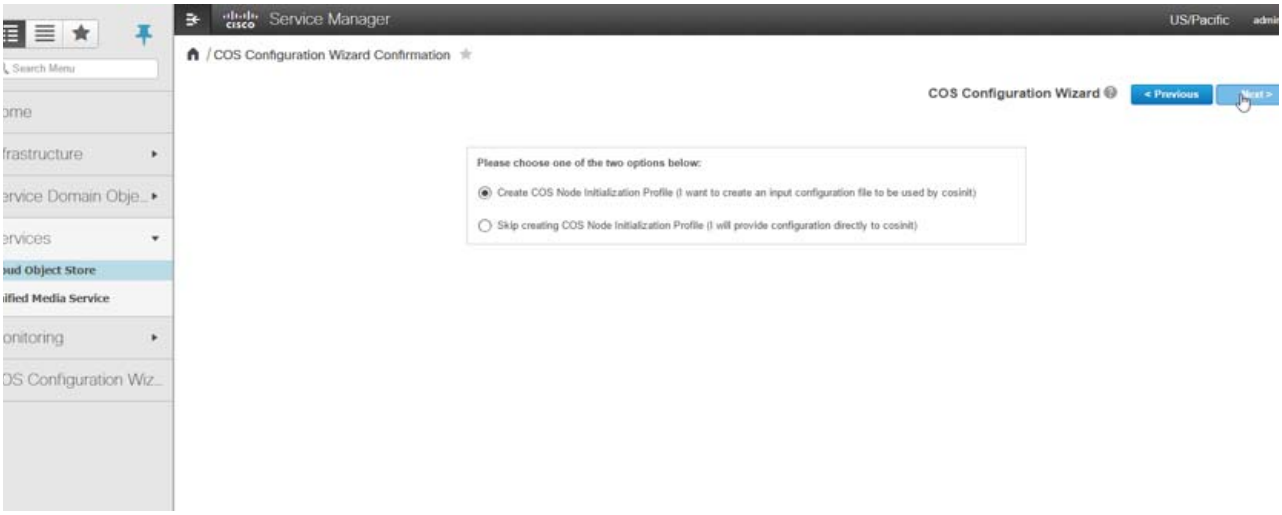
7. Specify Service Definition and Endpoint values, then click the **Admin State** drop-down and choose **Enable**. Save your settings then click **Next.**



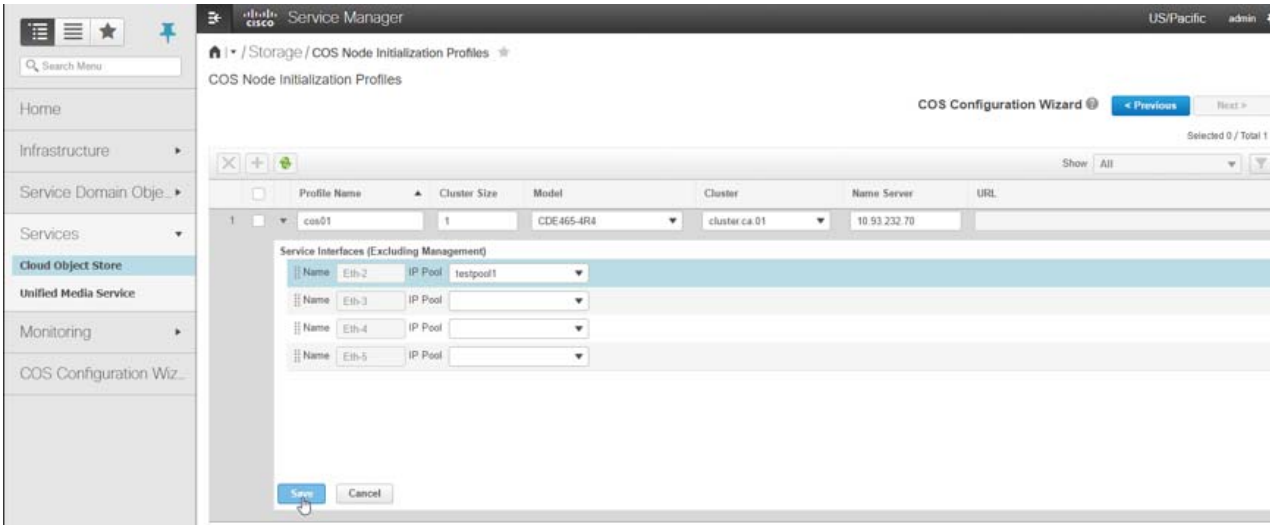
8. The Wizard Confirmation window appears.



9. Choose the option to create a cosinit script, otherwise this will need to be entered manually on the COS nodes during initialization.



10. Add an initialization profile and define the values, including model # and cluster. Interface designations will appear based on the Model selection. Define the IP pools to be used for each data interface (not management interface). Then click **Save.**



11. After clicking **Save,** a popup window will appear with the download URL for the cosinit script. The url will also appear in the Initialization Profiles window.

12. Copy the url into a browser to download the cosinit script from the PAM.

Configuring COS Service Instance

To add, delete, or edit Cloud Object Store, select **Services> Cloud Object Store** in the VMP Service Manager GUI. The COS service asset work flow attributes (Auth Profile, Asset Redundancy and State) are now merged into the new service endpoints. Multiple endpoints can be added to a COS service definition as well as the ability to edit and delete endpoints.

The Cloud Object Store table displays the following information for the COS Service Definition.

- Title– The title of the COS Service. The default title is **An unused COS service**.
- Description–Description of the COS service.
- Admin State– The administrative state of the COS service. From the drop-down list, you can choose to enable or disable the service.
- Service Template– Currently, this read only field identifies the default service template, **Cisco Object Store (COS) Service.**

The following parameters are displayed for the Service Endpoints.

- Name– The name of the service endpoint. Multiple endpoints can be added to a COS service definition.
- Description– A brief description of the service endpoint.
- Region– The region to which the service endpoint belongs.
- Min Nodes– The minimum number of nodes that must be associated with the service endpoint.
- Desired Nodes– The desired number of nodes for the service endpoint.
- Max Nodes– The maximum number of nodes that can be associated with the service endpoint.
- Max Storage– The maximum storage associated with the endpoint.
- Cluster Name– The service endpoint can have multiple clusters.
- AuthProfile– The default value is auth-1.
- Asset Redundancy Policy– The resiliency method for the service endpoint. The default value is redundancy-pol-cos.
- State-The state of the service endpoint.

Configuring COS Clusters

A COS Cluster is a grouping of COS nodes with a unique name.

To add, delete, or edit COS Nodes, select **Infrastructure > Storage > COS Cluster** in the VMP Service Manager GUI.

The COS Clusters table displays the following information for each configured cluster.

- Name–Name of the COS Cluster.
- Description–Description of the COS Cluster.
- Region–A region is made up of one or more zones. It can be associated with one or more geographical regions or data centers. This release supports a single region.
- Authentication FQDN–The Domain name for the COS authentication requests.
- Storage FQDN–The Domain name for the COS authentication requests.

Configuring COS Container Stores

To add, delete, or edit COS stores, select I**nfrastructure > Storage > COS Container Stores** in the VMP Service Manager GUI.

The COS Stores table displays the following information for each configured COS store:

- Name—Name of the COS store (required). The name is a string of up to 30 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Description—Description of the COS store. The description is a string of up to 100 characters, and can include uppercase or lowercase letters, numbers, and any special characters.
- Container— Defines a namespace for objects.
- Auth Profile— The default value is **auth-1.**

Configuring COS Node Initialization Profiles

You can automate the node configuration by providing a file to the COS initialization routine that includes a cluster name and IP pool reference address for at least one service interface. COS initialization will then configure the node without further intervention through the GUI or the API. A single configuration file for all COS nodes (or node sets) can be stored on an HTTP server for download by COS. Beginning with COS 3.12.1, the COS Node Profile page of the V2PC GUI can be used to configure a profile template for automated configuration of COS Nodes. Using such a configuration template avoids the need to configure files individually for each COS node.

The COS Node Initialization Profiles table displays the following information:

- Profile Name— Name of the COS Node Initialization Profile (required). The name is a string of up to 63 characters. Acceptable characters include uppercase letters and hyphens and lowercase letters and hyphens (-). The name must begin with a letter, and it is not case-sensitive.
- Cluster Size— Cluster size for the profile. Cluster size should be greater than zero.
- Model— Model For profile. Valid values are “CDE470-4R2”,”CDE465-4R4”,” UCSC-C3160-4U1”,” UCSC-C3160-4U2”,”UCSC-C3260-4U3 (28 6TB Drives)”,”UCSC-C3260-4U4 (56 6TB Drives)”,” UCSC-C3260-4U5 (28 10TB Drives)”, UCSC-C3260-4U6 (56 10TB Drives).
- Cluster— Cluster for the profile. Cluster will be listed in this field. User needs to select a cluster.
- Name Server— Name server for the profile. Name server is the IP address field. This field only accepts IPv4 files.
- URL— URL is a non-editable field. Once the Profile is saved, the URL will be generated and populated.

The Services Interfaces table will display based on your model selection with the following parameters.

- Name— Interface name- non-editable field
- IP Pool— IP Pool for interface. at least one IP pool must be selected for the model.

Configuring File System Gateway (FSG) Tenant

The Cisco Filesystem Gateway (FSGW) for Cisco Cloud Object Storage (COS) is an available option for COS 3.8.1 and later releases. While earlier COS releases allowed access only to object storage, the FSGW option gives COS the ability to access files using Network File System (NFS) or Common Internet File System (CIFS), the two main file systems used by network attached storage (NAS). NFS and CIFS are the client-server file systems used by the Linux and Windows operating systems, respectively. Adding FSGW enables COS to manage storage for existing Linux or Windows NAS media libraries directly, without the need to first convert these libraries to object data, thus improving COS utility and deployment speed.

The FSG Tenant table displays the following information:

- Name– Name of the FSG Tenant (required). The name is a string of up to 63 characters. Acceptable characters include uppercase and lowercase letters and hyphens (-). The name must begin with a letter, and it is not case-sensitive
- Description– Description of the FSG Tenant. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
- Auth Profile- Auth Profile for the FSG Tenant (required). Auth Profile will be listed in this field. User need to select one.
- Tenant PAM (Domain)–Domain for the Tenant (required). The Tenant PAM (Domain) is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
- Initial Password– Password for the FSG Tenant (required). The Initial Password is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
- Storage Size– Storage size for the FSG Tenant (required). Storage size should be greater than zero.

The COS Cluster and File System Gateway Nodes table will be displayed with the following parameters.

- COS Cluster– COS Cluster for the FSG Tenant (required). Cluster will be listed. At least one cluster should be selected for the FSG Tenant.
- FSG–FSG for the FSG Tenant (required). FSG will be listed. At least one FSG should be selected for the FSG Tenant

.Configuring NAS Stores

To add, delete, or edit NAS stores, select **Infrastructure > Storage > NAS Stores** in the VMP Service Manager GUI.

The NAS Stores table displays the following information for each configured NAS store:

- Name–Name of the NAS store (required). The name is a string of up to 30 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Description–Description of the NAS store. The description is a string of up to 100 characters, and can include uppercase or lowercase letters, numbers, and any special characters.
- Share Path–Share path used by the NAS store on the network.
- NFS Version–Version of the Network File System (NFS) used by the NAS store. Valid versions are **3.0** and **4.0**.

To display the range of servers available to the NAS store, click its **Expand** arrow.

- Make sure you specify start and end IP address ranges for the servers.
- The first three bytes of the Start IP Address must match those of the End IP Address. For example, 1.1.1.1 to 1.1.1.2 is valid start and end IP address range, but not 1.1.1.1 to 1.1.2.2.
- For a single server, the Start IP Address and the End IP Address are the same.

Click the **Collapse** arrow to collapse the image information.

Editing Platform Services

To work with NTP servers, DNS servers, DNS forwarders, and the Platform Service Instance, select **Infrastructure > Platform Services** in the VMP Service Manager GUI. The Platform Services page is displayed.

NTP Servers

The NTP Servers table displays the following information for each NTP server:

- Name—Name of the NTP server (required). The name is a string of up to 30 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Description—Description of the NTP server. The description is a string of up to 100 characters, and can include uppercase or lowercase letters, numbers, and any special characters.
- Region—Region in which the NTP server resides.

The NTP servers are configured automatically when the PAM is deployed. You can edit the Description, Region, and Servers for an NTP server, but you cannot add or delete NTP servers from this page.

DNS Servers

The DNS Servers table displays the following information for each DNS server:

- Name—Name of the DNS server (required). The name is a string of up to 35 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Description—Description of the DNS server. The description is a string of up to 100 characters, and can include uppercase or lowercase letters, numbers, and any special characters.
- Region—Region in which the DNS server resides.
- IPv4 Address—IPv4 address of the DNS server.
- Domain— location of the DNS server.
- TSIG Algorithm—Name of the TSIG algorithm used by the DNS server.

The DNS servers are configured automatically when the PAM is deployed. You cannot add, delete, or edit DNS servers from this page.

DNS Forwarders

The DNS Forwarders table displays the following information for each DNS forwarder:

- Name—Name of the DNS forwarder (required). The name is a string of up to 35 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Description—Description of the DNS forwarder. The description is a string of up to 100 characters, and can include uppercase or lowercase letters, numbers, and any special characters.
- Region—Region in which the DNS forwarder resides.
- IPv4 Address—IPv4 address of the DNS forwarder.
- Domain—Domain name of the DNS forwarder.

The DNS forwarders are configured automatically when the PAM is deployed. You can edit the Description, Region, IPv4 Address, and Domain for a DNS forwarder, but you cannot add or delete DNS forwarders from this page.

Platform Service Instance

PAM Endpoints

The Pam Endpoints table displays the following information:

- Name—Name of the PAM endpoint
- Region—The region to which the service endpoint belongs.
- Description—Description of the service endpoint

PAM Nodes

The PAM Nodes table displays the following information:

Note: Only the Edit and Refresh options are available.

- Name—Name of the node (required). You cannot edit this field.
- Description—Description of the node. You cannot edit this field.
- Zone—Zone with which the node is associated. You cannot edit this field.
- Image Version—Image version number. You cannot edit this field.
- Personality—Personality of the image associated with the node. You cannot edit this field.
- Admin State—Administrative status of the node. Valid values are **Inservice** and **Maintenance**. This is the only field that can be edited.
- Operation State— Operational status of the node. You cannot edit this field.
- Fault Status—Fault state of the node. You cannot edit this field.
- Fault Description—Description of the fault. You cannot edit this field.

Logging Endpoints

The logging endpoints table displays the following information:

- Name—Name of the logging endpoint
- Region—The region to which the logging endpoint belongs.
- Description—Description of the logging endpoint

Configuring Software Image Manifests

The VMP software images are used to create the services. You can assign different software image manifests to different services.

Note: Before setting a service instance to **Enabled**, you must configure at least one image manifest and associate it with the service instance.

To add, edit, or delete VMP software image manifests, (images for the service instance), select **Infrastructure > Software Image Manifests** in the VMP Service Manager GUI.

The Software Image Manifests page displays the following information for each manifest:

- Name—Name of the image manifest (required). The name is a string of up to 35 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Description—Description of the manifest. The description is a string of up to 100 characters, and can include uppercase or lowercase letters, numbers, and any special characters.

To display the images in a manifest, click its **Expand** arrow.

- The Images table displays the following information for each image:
  - Application Type—Type of VMP software image. Valid values are **MCE**, **App Engine**, and **MPE**.
  - Version—Version of the image. Default values are **2.5** (for MCE) and **2.5** (for MPE and App Engine).

  The image version for a software image manifest must match the version configured in the associated node. For more information, see the Configuring VMP Nodes, page 78.
- To add, delete, or edit the images for a manifest, select the manifest and click **Edit** at the top of the table.
  - Click **the + button** in the Images table to add an image.
  - Select an image and click **X** in the Images table to delete the image.
  - Select an image and click the **Edit**  icon in the Images table to edit the image.
- Click the **Collapse** arrow to collapse the image information.

Displaying and Configuring Regions and Zones

A zone is a set of Cloud platform components (compute, network, storage, and security) that are fate-shared. The zone can be mapped to the underlying Cloud platform provider, such as a datacenter in vCenter, an Availability Zone, or any other combination of fate-shared Cloud resource topologies. Each zone is associated with one Cloud Controller.

A region is made up of one or more zones. It is an abstract representation of the underlying Cloud platform. A region can be associated with a geographical region, one or more data centers, or a service area.

To display VMP regions, and to add, edit, or delete zones associated with those regions, select **Infrastructure > Regions & Zones** in the VMP Service Manager GUI.

The Regions & Zones table displays the following information for each region:

- Region Name—Name of the region. You cannot edit this field.
- Description—Description of the region. You cannot edit this field.
- Controllers—Controllers associated with the region. You cannot edit this field.

  The controller information defines the location (vCenter server) in which the VMP VMs are to be deployed and administered, and the hosts to be used. After you define the controllers, the VMP discovers the hosts that are administered by the controllers.

To display the zones associated with a region, click its **Expand** arrow.

- Name—Name of the zone (required). The name is a string of up to 63 characters. Acceptable characters include uppercase and lowercase letters and hyphens (-). The name must begin with a letter, and it is not case-sensitive.
- Description—Description of the zone.

- Click the **Collapse** arrow to collapse the Zones table for a region.

Configuring Channels

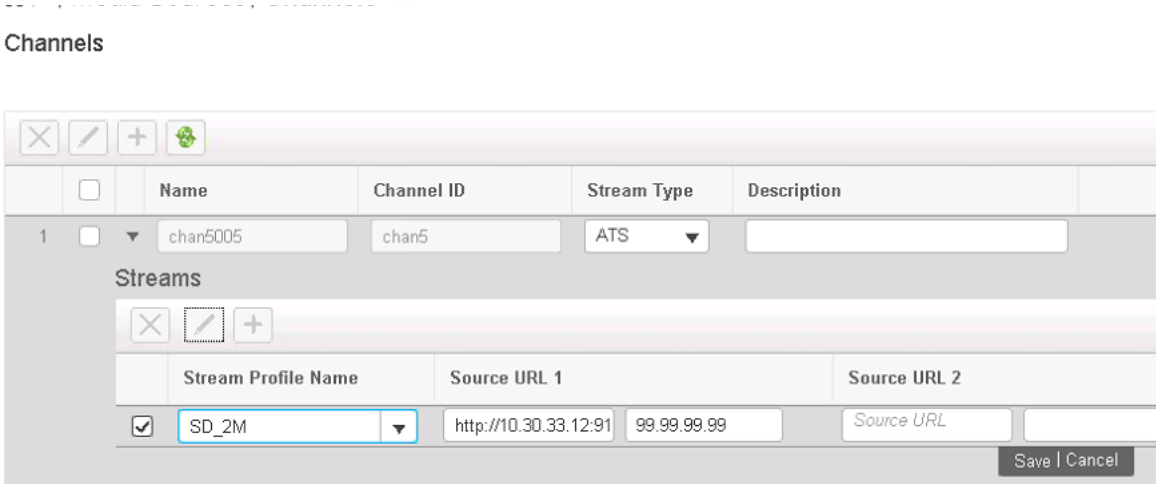
Channel configuration is valid only for Live service instances.

To add, edit, or delete channels, as well as the video streams associated with those channels, select **Service Domain Objects > Media Sources > Channels** in the VMP Service Manager GUI.

The Channels table displays the following information for each configured channel:

- Name—Name of the channel (required). The name is a string of any length. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Channel ID—ID of the channel (required). The ID is a string of up to 20 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The ID must not begin with a period (.), and it is not case-sensitive.
- Stream Type—Type of stream associated with the channel.
- Description—Description of the channel. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.

To display the streams associated with a channel, click its **Expand** arrow.



The Streams table displays the following information for each stream:

- Stream Profile Name—Name of the stream profile associated with the channel.
- Source URL 1 through 4—Multicast and unicast URLs associated with the stream.
- Source URL 2 through 4— Multicast and unicast URLs associated with the stream.

To add a stream to the Streams table:

1. Click **the + button**.
2. Select a video profile from the drop-down box.

- Valid profiles are **SD_2M** and **HD_4M**.
- The encoding type must be **H.264/AAC** (the default).
- The default bitrates are **2000000 bps** for SD_2M and **4000000 bps** for HD_4M. To change the bitrate for a stream profile, in the Stream Profiles popup, select the profile and click **Edit**. (You cannot change the encoding type for a stream profile.)
- To add a profile, click **the + button**. You can add any number of unique profiles to a given channel.

3. Associate one or more multicast or unicast groups with the stream by entering a Source URL (required) and Source IP Address (optional) for each multicast or unicast group.

The following formats are valid Source URLs:

http://*url*
udp://*url*

where *url* is a string of 50 characters, and can include uppercase or lowercase letters, numbers, and any special characters except commas (,) and semicolons (;).

If you enter a Source IP Address, the GUI performs IPv4 validation on it.

For a unicast group, use the following format for the Source URL:

udp://0.0.0.0:*source_port*

Example:

udp://0.0.0.0:12000

The MCE recognizes IP address **0.0.0.0** as itself and reads the data from all of its interfaces on the *source_port*.

4. To save the new stream, click **Save**.
5. To cancel at any time, click **Cancel**.

Click the **Collapse** arrow to collapse the stream information.

Configuring NAS Media Sources

The VMP uses the NAS media source to read VOD source files for VOD ingest.

NAS media source configuration is valid only for VOD service instances.

To add, edit, or delete NAS media sources, select **Service Domain Objects > Media Sources > NAS Media Sources** in the VMP Service Manager GUI.

The NAS Media Sources table displays the following information for each NAS media source:

- Name—Name of the NAS media source, or content library (required). The name is a string of 30 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Description—Description of the NAS media source. The description is a string of 30 characters, and can include uppercase or lowercase letters, numbers, and any special characters.
- Share Path—Share path used by the NAS media source on the network (required).
- NFS Version—Version of the Network File System (NFS) used by the NAS media source. Valid versions are **3.0** and **4.0**.

To display the range of servers available to the NAS media source, click its **Expand** arrow.

- Make sure you specify start and end IP address ranges for the servers.
- The first three bytes of the Start IP Address must match those of the End IP Address. For example, 1.1.1.1 to 1.1.1.2 is valid start and end IP address range, but not 1.1.1.1 to 1.1.2.2.
- For a single server, the Start IP Address and the End IP Address are the same.

Click the **Collapse** arrow to collapse the range of servers.

Configuring Dynamic Sources

Use the following procedure to set up a capture only cDVR capture workflow.

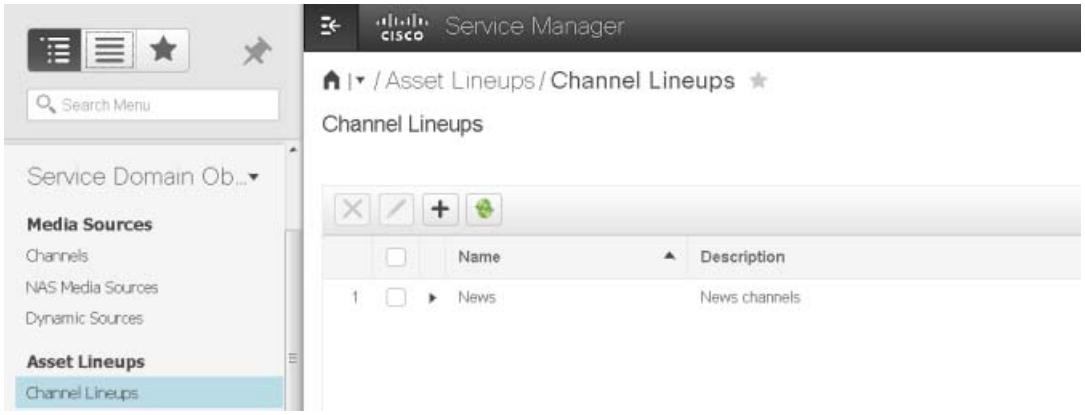
1. Select **Service Domain Objects>Media Sources>Dynamic Sources** to display the Dynamic Sources page.

2. **A**dd a new Dynamic media source by clicking the **+** button, or edit an existing media source by selecting it and clicking the **Edit**  icon.

Configuring Channel Lineups

Channel lineup configuration is valid only for Live service instances.

To add, edit, or delete channel lineups, select **Service Domain Objects > Asset Lineups > Channel Lineups** in the VMP Service Manager GUI.

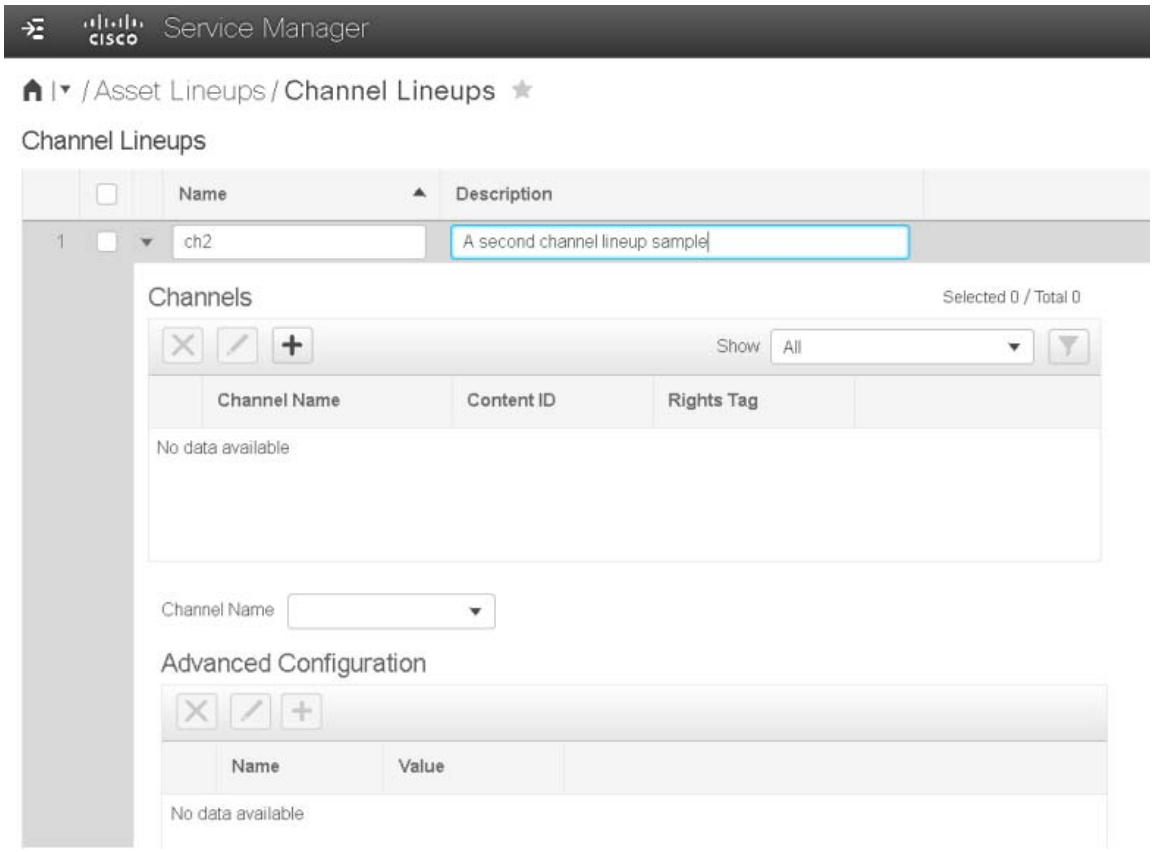


The Channel Lineups table displays the following information for each channel lineup:

- Name—Name of the channel lineup (required). The name is a string of up to 30 characters. Acceptable characters include uppercase and lowercase letters and numbers. No special characters are allowed. The name is not case-sensitive.
- Description—Description of the channel lineup. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.

To add a channel lineup to the Channel Lineups table, click **the + button**. To edit a channel lineup, select it and click the **Edit icon**.

To display the channels associated with a channel lineup, click its **Expand** arrow.



- The Channels table displays the following information for each channel associated with the channel lineup:
  - Channel Name—Name of the channel. You cannot edit this field.
  - Content ID—Content ID of the channel. The ID is a string of any length. Acceptable characters include uppercase and lowercase letters, numbers, and underscores (_). The user ID must not begin with a period (.), and it is not case-sensitive.
  - Rights Tag—Tag used to drive the asset redundancy policy tag match. The tag is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
  - Advanced Configuration—If there are any configuration details associated with a channel, they are displayed in the Advanced Configuration table when the channel is selected. The table displays the Name, validated by regular expression (regex), and the Value for the channel. A channel can have more than one set of acquisition details.

  To enable content ID mapping (mandatory), add one or more sets of configuration details to the Advanced Configuration table for a channel. To do so, select the channel, click **the + button** and enter the name and value for the channel.
- To collapse the channel information, click the **Collapse** arrow.

To add channels to a new channel lineup, click the double arrows in the Channels table, then click **the + button**. The Add Channel popup displays the following information:

- Available Channels—Channels that are available to be added to the channel lineup. For more information about channels, see the Configuring Channels, page 93.

- Selected Channels—Channels that are currently in the channel lineup.

  For each channel, the Selected Channels displays the Channel Name, Content ID, and Rights Tag. To edit these fields, select the channel and click **Edit**.

Add one or more of the available channels to the channel lineup by selecting the channels in the Available Channels list and using the right-arrow to move them into the Selected Channels list. You can associate a channel with more than one channel lineup.

To remove one or more channels from the new channel lineup, select the channels in the Selected Channels list and use the left-arrow to move them back into the Available Channels list.

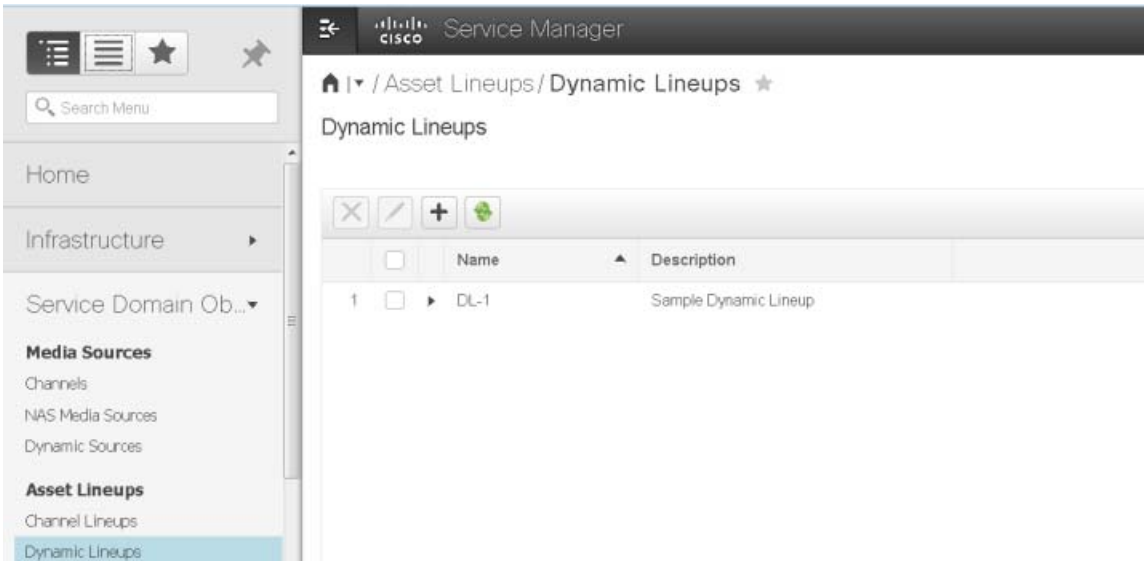
When you are satisfied with the name, description, and selected channels for the new channel lineup, click **Save**.

To cancel at any time, click **Cancel**.

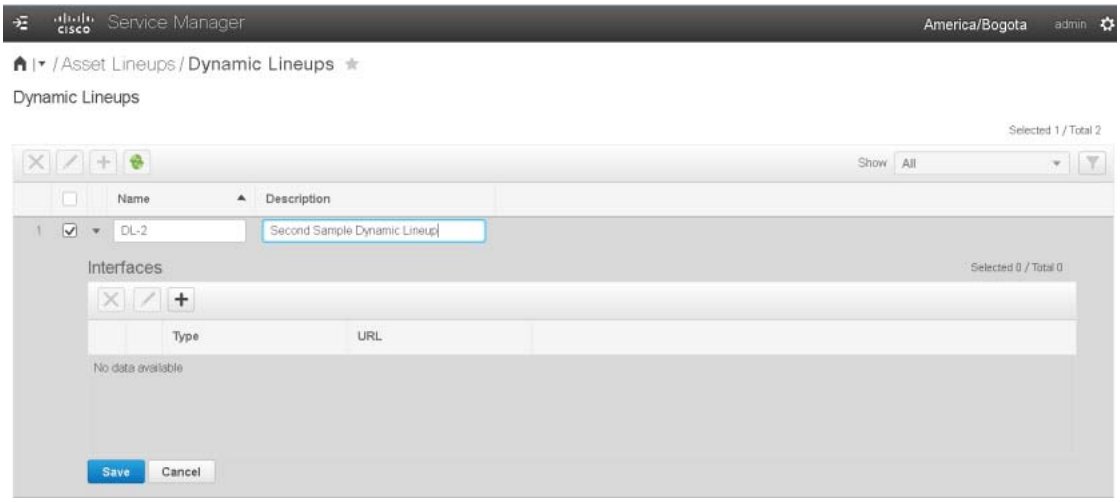
Configuring Dynamic Lineups

Dynamic linesups are the input source for cDVR workflows. Use the following procedure to set up a Dynamic line up.

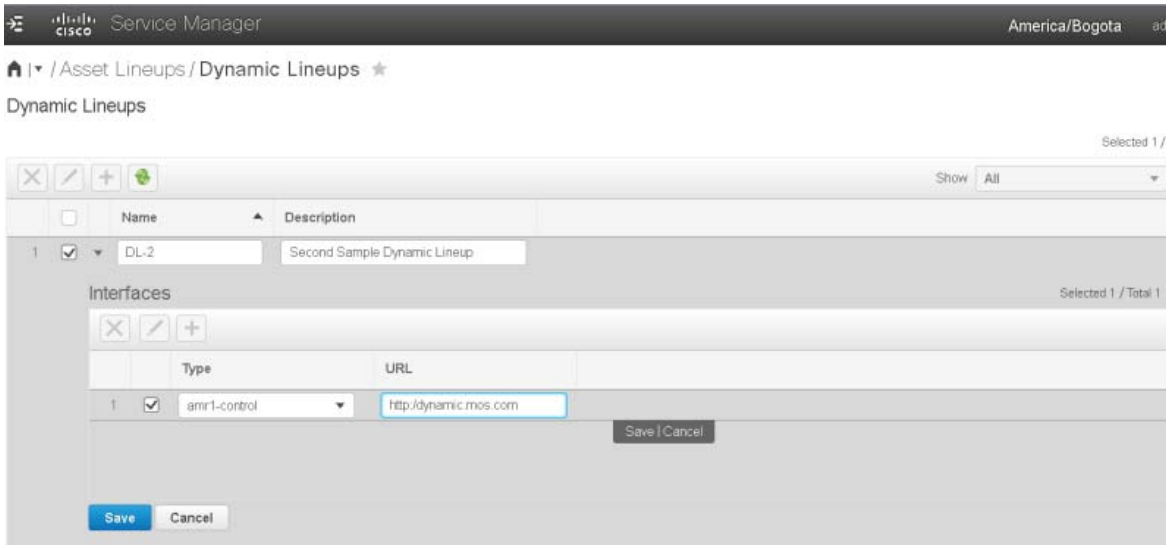
1. To add, delete, or edit Dynamic lineups, select **Service Domain Objects> Asset Lineups> Dynamic Lineups** to display the Dynamics Lineups page.



2. Add a new dynamic lineup by clicking the **+** button, or edit an existing dynamic lineup by selecting it and clicking the **Edit** icon.



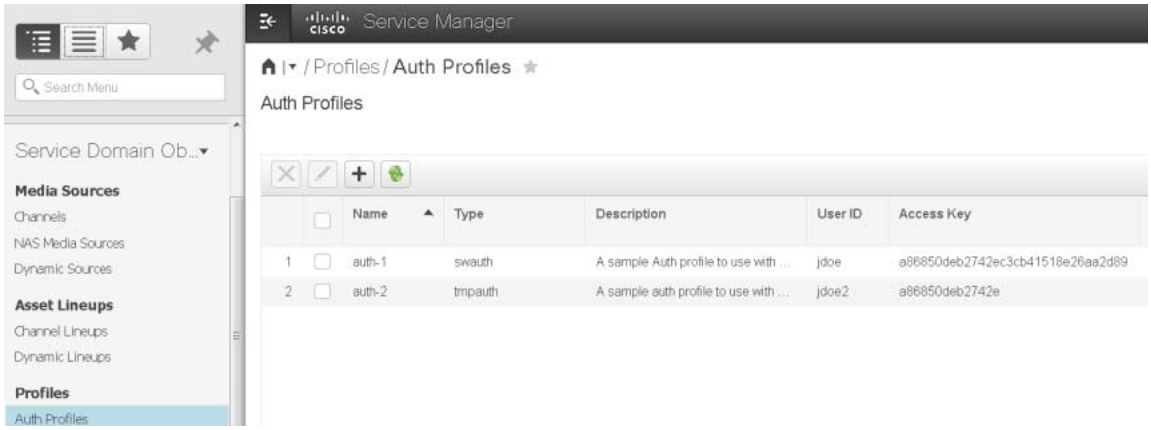
3. Add interfaces to a dynamic lineup by clicking the **+** button, or edit an existing interface by selecting and clicking the **Edit** icon. One can configure the recorder manager control interface url (a.k.a amr1-control interface)



Configuring Auth Profiles

Auth Profiles are authorization profiles that point to an auth provider. Use the following procedure to set up Auth profiles.

1. To add, delete, or edit Auth profiles, select **Service Domain Objects > Profiles > Auth Profiles** to display the Auth Profiles page.



2. Click the **+** button to add Auth profiles as needed.

Configuring ESAM Profiles

The Event Signaling and Management (ESAM) profiles define how the VMP is to handle ESAM multi-screen ad insertion.

To add, delete, or edit ESAM profiles, select **Service Domain Objects > Profiles > ESAM Profiles** in the VMP Service Manager GUI.

The ESAM Profiles table displays the following information for each configured key profile:

- Name—Name of the ESAM profile (required). The name is a string of any length. Acceptable characters include uppercase and lowercase letters, numbers, and underscores (_). The user ID must not begin with a period (.), and it is not case-sensitive.
- POIS URL—Placement Opportunity Information System (POIS) URL of the ESAM server.(Required field)
- Description—Description of the ESAM profile. The description is a string of up to 235 characters, and can include uppercase or lowercase letters, numbers, and any special characters.
- Version—Version of the ESAM profile. Select a version from the drop-down box. Valid versions are **OC-SP-ESAM-API-I01** and **OC-SP-ESAM-API-I03**.

Configuring Key Profiles

The key profiles define how the VMP is to perform encryption.

To add, delete, or edit key profiles, select **Service Domain Objects > Profiles > Key Profiles** in the VMP Service Manager GUI.

The Key Profiles table displays the following information for each configured key profile:

- Name—Name of the key profile (required). The name is a string of up to 200 characters. Acceptable characters include uppercase and lowercase letters, numbers, and underscores (_). The user ID must not begin with a period (.), and it is not case-sensitive.
- KMS Type—KMS type used by the key profile. Valid KMS types are:
  - Adobe License Server; supports DRM type Adobe-Access
  - Advanced Encryption Standard (AES)
  - Irdeto; supports DRM types HLS-AES-128 and PR-AES-128
  - Key Store; supports DRM type HLS-AES-128
  - Verimatrix; supports DRM types HLS-AES-128 and PR-AES-128
  - Insys; supports DRM types PR-AES-128
  - VGC; supports DRM types HLS-AES-128 and PR-AES-128
  - Nagra; supports DRM types HLS-AES-128
  - Fairplay; supports DRM type Fairplay_AES-128
- DRM Type—DRM type used by the key profile. Valid DRM types are:
  - Adobe-Access, valid for KMS type Adobe License Server.
  - HLS-AES-128, valid for KMS types, Irdeto, Key Store, Verimatrix, and VGC
  - PR-AES-128, valid for KMS types Irdeto, Verimatrix, Insys, and VCG
  - CECC-DASH, valid for KMS types EZDRM snd BUYDRM
  - VGC-HLS, valid for VGC
  - WV-AES-CTR, valid for Insys
- Description—Description of the key profile. The description is a string of up to 235 characters, and can include uppercase or lowercase letters, numbers, and any special characters.

To add a key profile to the Key Profiles table, click the **+** button and enter or select values for the profile.

Make sure you also enter values for the following fields:

- Transport Certificate—(Optional) Name of the certificate file used to secure communication between clients and the Adobe license server.

  Valid for the **Adobe License Server** KMS type.
- License Certificate—(Optional) Name of the certificate file used to assign content licenses to clients.

  Valid for the **Adobe License Server** KMS type.

- License Server URL—(Optional) URL of the Adobe license server.

  Valid for the **Adobe License Server** KMS type.

- Policy—(Optional) name of the policy used to package content.

  Valid for the **Adobe License Server** KMS type.

- Packager Certificate—(Optional) Name of the certificate file used to encrypt content.

  Valid for the **Adobe License Server** KMS type.

- Packager Passcode—(Optional) Passcode used with the packager certificate.

  Valid for the **Adobe License Server** KMS type.

- DRM Key Provider—Name of the key provider that distributes active keys to clients.

  Valid for the **Adobe License Server** KMS type.

- Key Service URI—Key service URI used to acquire the key profile (optional).

  Valid for the **Verimatrix**, **Key Store**, **Irdeto** and EZDRM KMS types.

- Client Certificate—(Optional) Client authentication certificate used to acquire the key profile. Enter the full path to the client certificate .crt file on the PAM. Do not enter the actual client certificate name.

  Valid for the **Verimatrix**, **Key Store**, and **Irdeto** KMS types.

- CA Certificate—(Optional) CA authentication certificate used to acquire the key profile. Enter the full path to the CA certificate .crt file on the PAM. Do not enter the actual CA certificate name.

  Valid for the **Verimatrix**, **Key Store**, and **Irdeto** KMS types.

- Client Key—(Optional) Client authentication key used to acquire the key profile. Enter the full path to the client key .key file on the PAM. Do not enter the actual client key name.

  Valid for the **Verimatrix**, **Key Store**, and **Irdeto** KMS types.

- Username—Username used to acquire the key profile (optional).

  Valid for the **Irdeto** and EZDRM KMS type.

- Passphrase—Passphrase used to acquire the key profile (optional).

  Valid for the **Irdeto** and EZDRM KMS type.

- Server Key—Server key used to acquire the key profile (optional)

  Valid for the BuyDRM KMS type

- User Key—User key used to acquire the key profile (optional)

  Valid for the BuyDRM KMS type.

- Account—Account ID used to acquire the key profile (optional).

  Valid for the **Irdeto** KMS type.

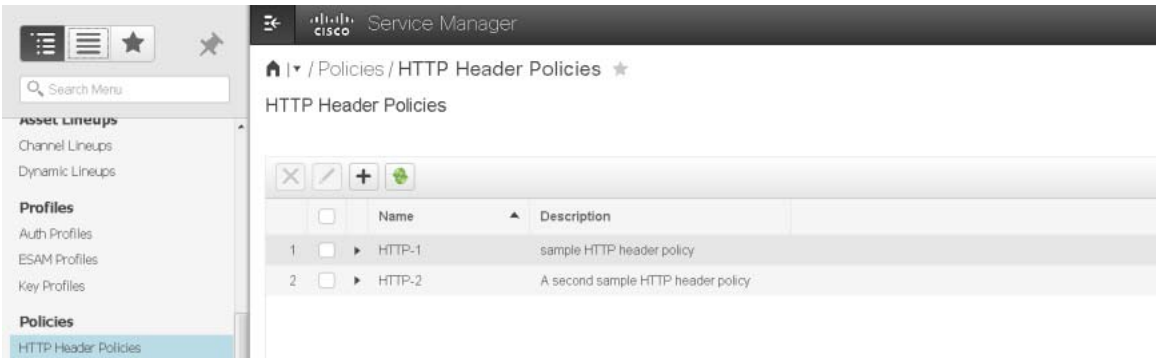
When finished, click **Save** to add the new profile to the Key Profiles table.

The Client Certificate, CA Certificate, and Client Key fields are optional. If you leave these fields blank, the SSL authorization check by the PAM's DRM system is bypassed when setting up an HTTPS connection to a KMS server.

Configuring HTTP Header Policies

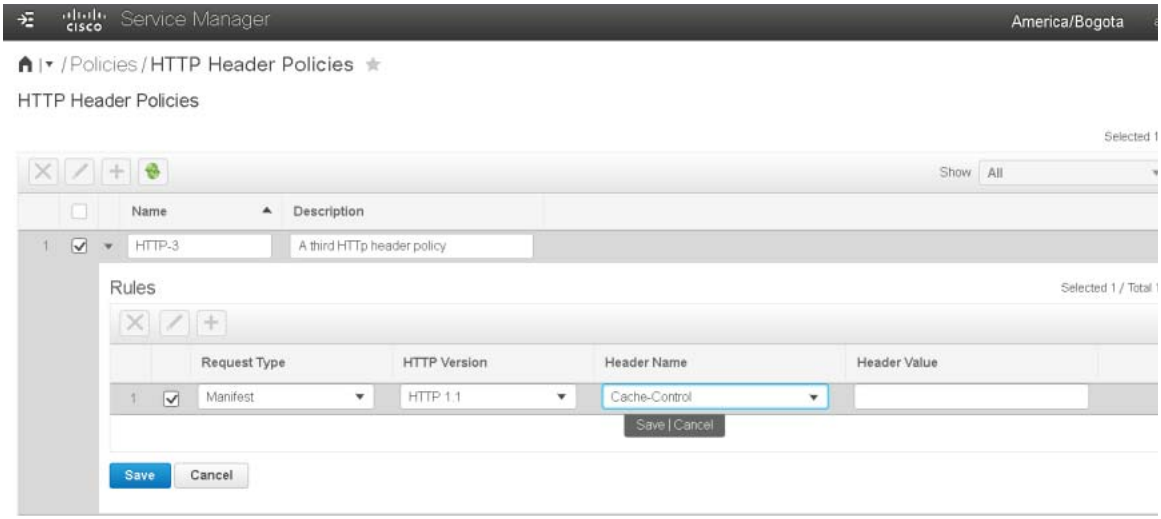
The HTTP header policies control the HTTP headers for publishing content.

To add, edit, or delete HTTP header policies, select **Service Domain Objects > Policies > HTTP Header Policies** in the VMP Service Manager GUI.



The HTTP Header Policies table displays the following information for each HTTP header policy:

- Name—Name of the HTTP header policy (required). The name is a string of any length. Acceptable characters include uppercase and lowercase letters and numbers. No special characters are allowed. The name is not case-sensitive.
- Description—Description of the HTTP header policy. The description is a string of 70 characters or more, and can include uppercase or lowercase letters, numbers, and any special characters. To display the rules associated with an HTTP header policy, click its **Expand** arrow.



- The Rules table displays the following columns for each rule:
  - Request Type—Indicates whether the rule is for a **Manifest** or **Chunk**.

    For a Live service, set Request Type to **Manifest**.
  - HTTP Version—Version of HTTP request. Valid value is **HTTP 1.1**.
  - Header Name—HTTP header name. Predefined headers are provided, but can be edited or modified.
  - Header Value—HTTP header value.

For a Live service, if Request Type is set to **Manifest** and HTTP Version is set to **HTTP 1.1**, then Header Name must be set to **Cache-Control** and Header Value must be set to **max-age=0**.

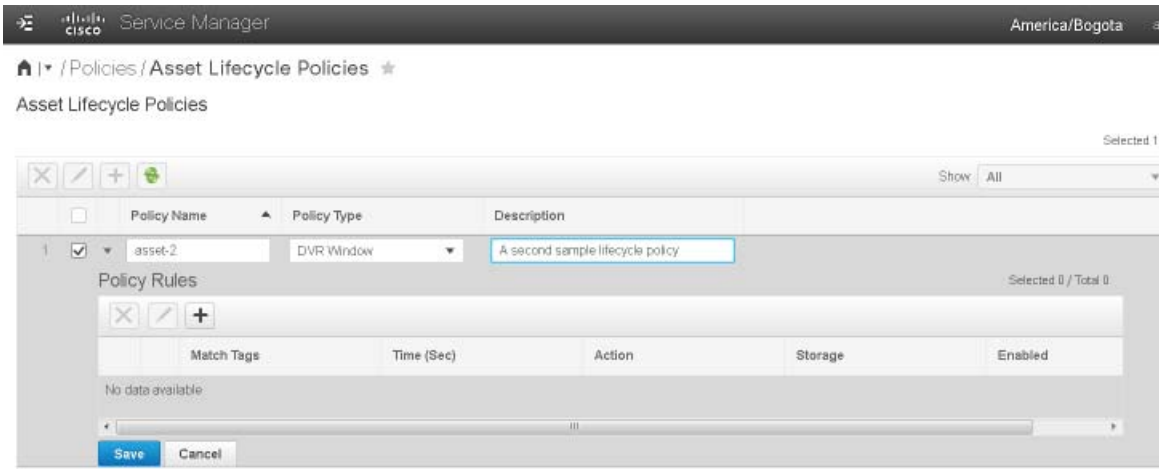
- Each HTTP header policy must contain at least one rule.
- Click the **Collapse** arrow to collapse the rule information.

Configuring Asset Lifecycle Policies

The VMP uses asset lifecycle policies to specify the Time-Shift TV (TSTV) window for Live capture.

Asset lifecycle policy configuration is valid only for Live service instances.

To add, edit, or delete asset lifecycle policies, select **Service Domain Objects > Policies > Asset Lifecycle Policies** in the VMP Service Manager GUI.



The Asset Lifecycle Policies table displays the following information for each asset lifecycle policy:

- Policy Name—Name of the asset lifecycle policy (required). The name is a string of 63 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Policy Type—Type of asset lifecycle policy. Valid value is **DVR Window**.
- Description—Description of the asset lifecycle policy. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.

To display the rules associated with an asset lifecycle policy, click its **Expand** arrow.

- The Policy Rules table displays the following columns for each rule:
  - Match Tags—Indicates whether the rule applies to the whole asset (**Asset**) or to a segment (**Segment**). **Segment** is required for a Live service.
  - Time—Time, in seconds, after which the specified action is to be taken.
  - Action—Action to apply to the asset or segment. Valid values are **Move** and **Purge.**
  - Storage—NAS store associated with the rule. For more information, see the Configuring COS Nodes, page 80.

  If the Action field is set to **Move**, the **Storage** field identifies the target storage.

  If the Action field is set to **Purge**, the **Storage** field is disabled.

  - Enabled—Indicates whether the rule is enabled. Valid values are **True** (enabled) and **False** (disabled).

- Click the **Collapse** arrow to collapse the rule information.

Configuring Asset Redundancy Policies

The VMP uses asset redundancy policies to specify the number of redundant copies of an asset to make. For example, if Number of Copies is set to **3**, the VMP creates copies of the asset on three separate MCE-Workers.

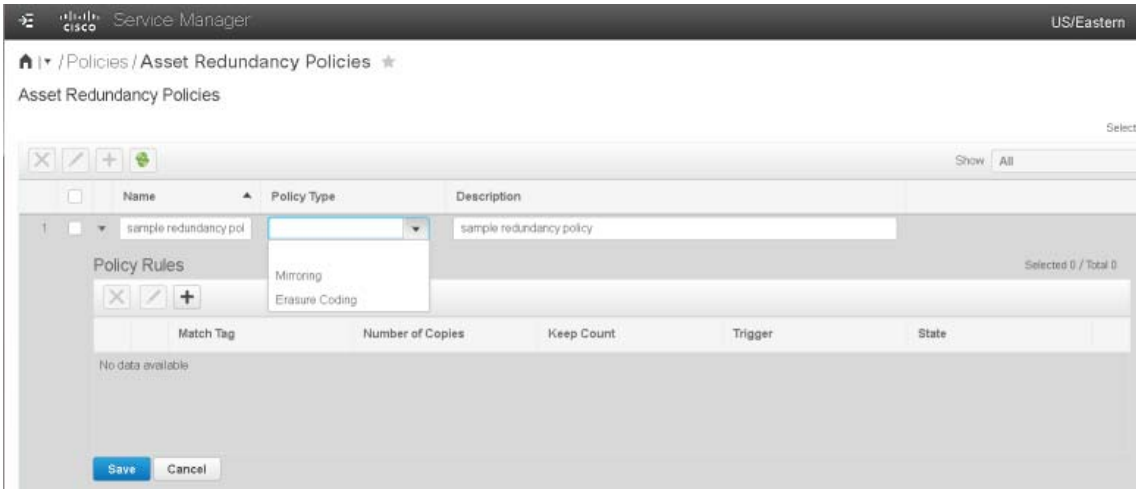
Asset redundancy policy configuration is valid only for Live and cDVR workflows.

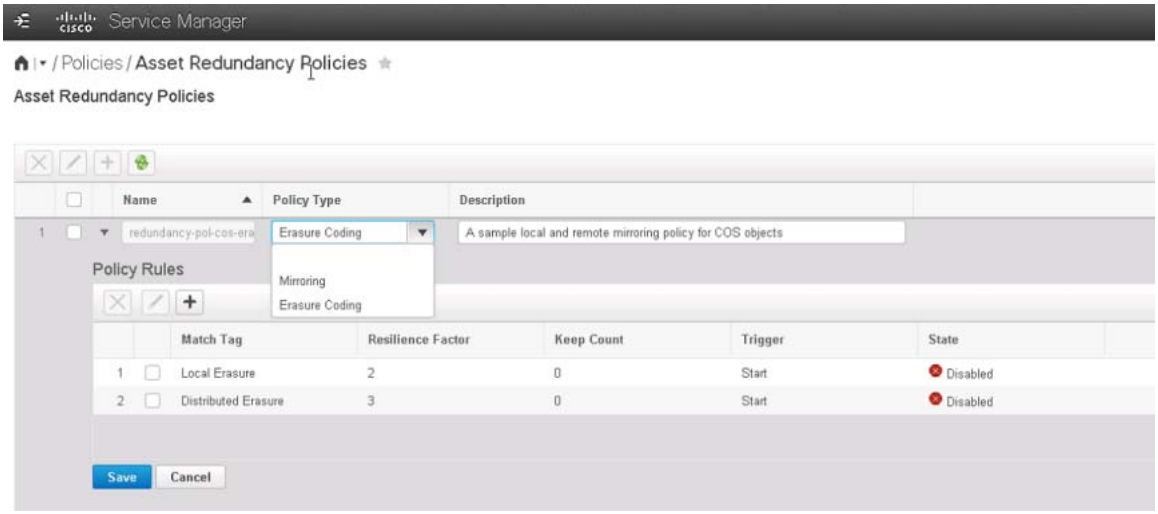
To add, edit, or delete asset redundancy policies, select **Service Domain Objects > Policies > Asset Redundancy Policies** in the VMP Service Manager GUI.

The Asset Redundancy Policies table displays the following information for each asset redundancy policy:

- Name—Name of the asset redundancy policy (required). The name is a string of any length. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Policy Type—Type of asset redundancy policy. The policy type does not apply to VMP. VMP now supports Mirroring or Erasure Coding policy types for COS objects.
- Description—Description of the asset redundancy policy. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.

To display the rules associated with an asset redundancy policy, click its **Expand** arrow. The rules displayed depends on the policy type selected. The below screens shows the rules for a non policy type (VMP) and the erasure coding policy type (COS).





- The Policy Rules table displays the following columns for each rule:
  - Match Tag– Indicates whether the rule applies to the whole asset or to a specific segment (required). Based on the values selected, the match tag changes. The above screen displays the Match tags for the Erasure Coding Policy type.
  - Number of Copies–Number of redundant copies to make (required). The valid ranges for Mirroring are: Local: 1-4 and Remote: 0-6.
  - Resilience Factor– (COS objects only) Specifies the number of simultaneous failures that can occur before data loss. This parameter is specific to the Erasure Coding Policy type. The valid ranges are: Local: 0-4 (0 means local EC disabled), Distributed: 0-4 (0 means Distributed EC disabled).
  - Keep Count– Keep accurate count of the assets available.
  - Trigger– Indicates whether the rule is started/completed
  - State–Indicates whether the rule is **Disabled** (the default setting) or **Enabled**.
- Click the **Collapse** arrow to collapse the rule information.

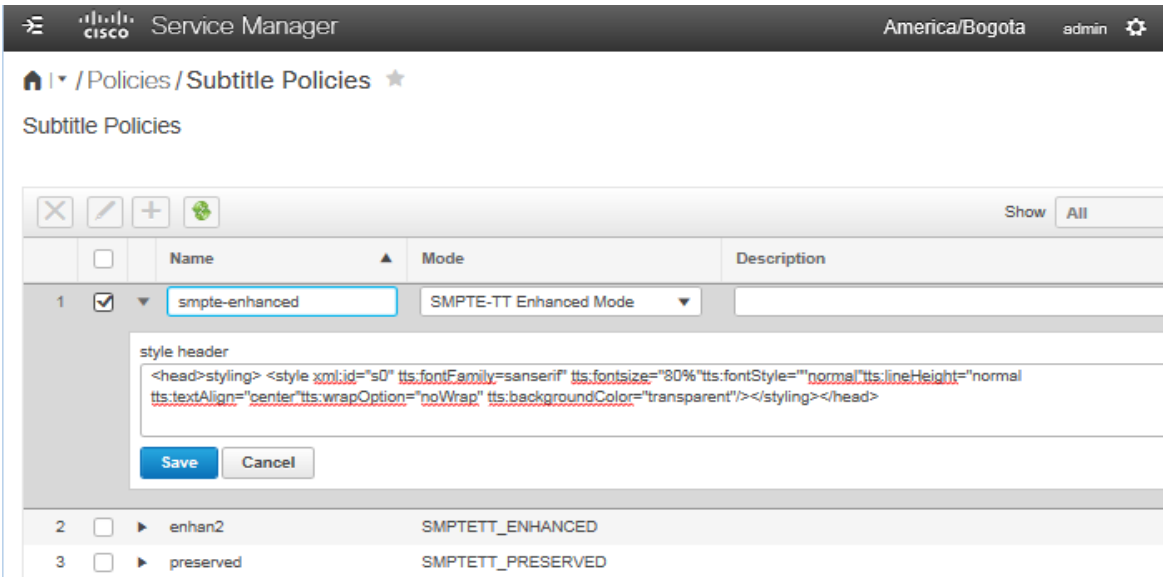
Configuring Subtitle Policies

The VMP uses Subtitle Policies to provide which subtitle style that can be used for DASH play out. When the user creates a publish template for DASH play out, it can be associated with a subtitle policy. Subtitle Policy is for DASH only. It is not supported by other ABR formats.

To add, edit or delete subtitle policies, select **Service Domain Objects > Policies > Subtitle Policies** in the VMP Service Manager GUI.The Subtitle Policies displays the following information for each subtitle policy.

- Name– Name of the subtitle policy (required). The name is a string of any length. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Mode–There are three subtitle policy modes:
  - SMPTE-TT Preserved Mode– In preserved mode, the subtitles from the media source will be correctly converted and rendered as accurate in a style of the original rendering as possible given the constraints of the formats. In preserved mode, the user do not need to configure the style header.
  - SMPTE-TT Enhanced Mode– In enhanced mode, the user can configure a customized display style header for DASH playout, e.g. visual effects, typography, coloring. The style header is a string in XML format. The attributes in the style header should conform to the specifications defined in the following document: https://www.smpte.org/sites/default/files/st2052-1-2010.pdf

  In the example screen shown below, the subtitles were configured to be displayed in this style: color is navy(#000080), font is sansSerif, font size is 80%, font style is normal, line height is normal, text align is center, wrap option is noWrap, background color is transparent.
  - TTML– TTML mode is similar to SMPTE-TT enhanced mode. The user can configure a customized style header, however the namespace in the subtitle XML files are TTML, therefore, the only attributes defined in this document: https://www.w3.org/TR/ttml2 are allowed to be configured in the style header input.
- Description– Description of the subtitle policy. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
- Style Header– Configure for DASH playout, e.g. visual effects, typography, coloring, etc.



Configuring Publish Templates

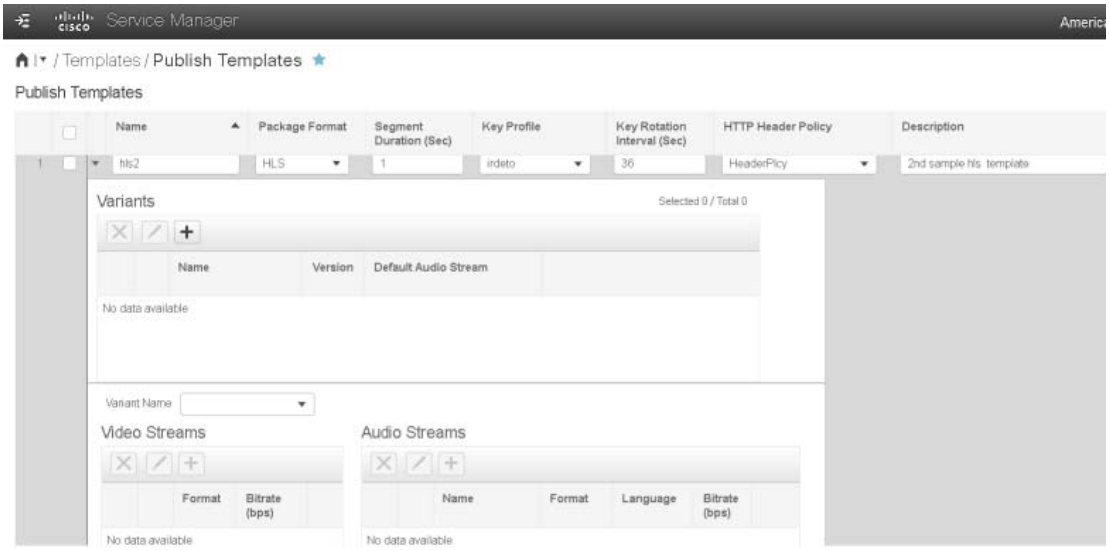
The publish template defines how the content is to be published.

To add, edit, or delete publish templates, select **Service Domain Objects > Templates > Publish Templates** in the VMP Service Manager GUI.

The Publish Templates table displays the following information for each template:

- Name—Name of the template (required). The name is a string of up to 63 characters. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Package Format—Package format supported by the template. Valid values are **HLS** (the default setting), **HSS, HDS, CIF, DASH-MP4 CIF-DASH-TS supported.**
- Segment Duration (Sec)—For segmented files, maximum time, in seconds, to write to a file before starting a new segment (required). The segment duration must match the Encoder Boundary Point (EBP) configured on the encoder, or it must be a multiple of the EBP value.
- Key Profile—Key profile associated with the template. For more information, see the Configuring Key Profiles, page 101.
- Key Rotation Interval (Sec)—Number of seconds to wait before using a new encryption key.
- HTTP Header Policy—HTTP header policy associated with the template. For more information, see the Configuring HTTP Header Policies, page 103.
- Description—Description of the template. The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.

To display the variants, video streams, and audio streams associated with a publish template, click its **Expand** arrow.



- The variants table enables you to provide a subset of video and audio bitrates to specific devices. For example, you can create a variant called **mac** and assign the top three bitrates to it, and create another variant called **ipad** and assign three lower bitrates to it.
- The Variants table displays the following columns for each variant:
  - Name—Name of the variant (required). The name is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
  - Version—Version of the variant (required). Valid versions are **2** through **5**. The default setting is **4**.
  - Order—Order of the variant. Two options are available:BITRATE and RANK. The manifest of this variant will include specified profiles ordered by BITRATE/RANK specified later.
  - Selective Publish—By default, the output manifest will not include profiles that are not specified. If the option is False, the system will append these profiles to the manifest.
  - Default Audio Stream—Name of the default audio stream associated with the variant.
- The Video Streams table displays the following columns for each video stream associated with the selected variant:
  - Format—Format of the video stream, such as **H264** (required).
  - Bitrate (bps)—The column is available when the order of the variant is BITRATE. The bitrate that you enter must be within 5% of an actual bitrate. The output manifest will include these profiles with the order user specified.
  - Rank—The column is available when the order of the variant is RANK. It is an integer that indicates the rank of the profile's bitrates in descending order. (1 = highest, 2 = 2nd highest, etc. The output manifest will include these profiles with the order user specified.
- The Audio Streams table displays the following columns for each audio stream associated with the selected variant:
  - Name—Name of the audio stream (required). The name is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
  - Format—Format of the audio stream, such as **AAC** (required).
  - Language—Language used for the audio stream, such as **en** for English (required).

  - Bitrate (bps)—Bitrate, in bps, supported by the variant for audio playback (required). The bitrate that you enter must be within 5% of an actual bitrate.

- To delete a variant, select it, then click **Delete**, then click **OK**.
- To delete a video or audio stream, select a variant, the select the stream, then click **Delete**, then click **OK**.
- To edit a variant, select it, then click **Edit**. Enter or select new values for the variant, then click **Save** to save the new values in the table.
- To edit a video or audio stream, select a variant, then select the stream, then click **Edit**. Enter or select new values for the stream, then click **Save** to save the new values in the table.
- To add a variant, click the **+ button**, enter or select values for the new variant, then click **Save** to add the variant to the table.
- To add a video or audio stream, select a variant, click the **+** button in the Video Streams or Audio Streams table, then enter or select values for the new stream. The video and audio bitrates must match those being sent from the encoder (within a 5% buffer). When finished, click **Save** to add the stream to the table.
- Click the **Collapse** arrow to collapse the variant information.

When configuring bitrates for video and audio streams, keep the following considerations in mind:

- The order in which you configure the bitrates is the order in which they are displayed in the manifest.
- The bitrates must be within 5% of an actual bitrate.
- If a configured bitrate is not within 5% of an actual output stream generated by a source, the VMP excludes that bitrate from the manifest.
- If none of the bitrates in a list is within 5% of an actual bitrate, the VMP generates a 404 error code when you request a manifest.
- If you do not specify a list of bitrates, then the VMP includes all of the bitrates generated by the source in the manifest.

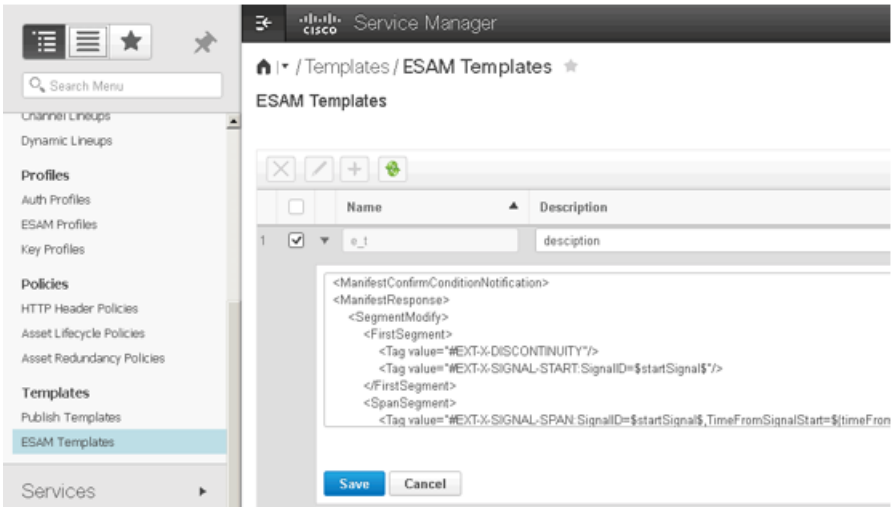
For example, if you have a Digital Content Manager (DCM) that generates video bitrates of 1MB, 2MB, 3MB, 4MB, and 5MB:

- You can configure video bitrates of 1 MB, 4 MB, and 5 MB to display them in the manifest in descending order, or of 5 MB, 4 MB, and 1 MB to display them in ascending order.
- If you configure 1.5 MB and 4 MB, only 4 MB is displayed in the manifest. 1.5 MB is not within 5% of an actual bitrate.
- If you configure 1.5 MB and 3.5 MB, the VMP generates a 404 error code because neither bitrate is within 5% of an actual bitrate.
- If you configure 1.05 MB and 2.9 MB, both 1 MB and 3 MB are displayed in the manifest because both are within 5% of an actual bitrate.

Configuring ESAM Templates

The Event Signaling and Management (ESAM) template define how the VMP is to handle ESAM multi-screen ad insertion.

To add, delete, or edit ESAM templates, select **Service Domain Objects > Templates> ESAM Template** in the VMP Service Manager GUI.



The ESAM Template table displays the following information for each configured key:

- Name—Name of the ESAM template (required). The name is a string of any length. Acceptable characters include uppercase and lowercase letters, numbers, and underscores (_). The user ID must not begin with a period (.), and it is not case-sensitive.
- Content—The content of ESAM template (required) It is provisioned by the service provider. See example below.
- Description—Description of the ESAM template. The description is a string of up to 235 characters, and can include uppercase or lowercase letters, numbers, and any special characters.

Content Example:

```
<ManifestConfirmConditionNotification>
<ManifestResponse>
  <SegmentModify>
    <FirstSegment>
      <Tag value="#EXT-X-DISCONTINUITY"/>
      <Tag value="#EXT-X-SIGNAL-START:SignalID=$startSignal$"/>
    </FirstSegment>
    <SpanSegment>
      <Tag value="#EXT-X-SIGNAL-SPAN:SignalID=$startSignal$,TimeFromSignalStart=${timeFromSignal}"/>
    </SpanSegment>
    <LastSegment>
      <Tag value="#EXT-X-SIGNAL-END:SignalID=$endSignal$"/>
      <Tag value="#EXT-X-DISCONTINUITY"/>
    </LastSegment>
  </SegmentModify>
</ManifestResponse>
</ManifestConfirmConditionNotification>
```

FirstSegment: The segment in playlist manifest which is the first one after out point.

LastSegment: The segment in playlist manifest which is the last one before in point.

SpanSegment: The segments in playlist manifest which between FirstSegment and LastSegment. (this Tag is optional)

$startSignal$: the signal ID from the out point command

$endSignal$: the signal ID from the in point command

${timeFromSignal}: the time from out point

Configuring Media Service

Refer to Configuring Media Service, page 112.

Configuring an Asset Workflow

Refer to Creating Asset Workflows, page 52

Displaying System Diagnostics

To display system diagnostics for the VMP, select **Monitoring > Diagnostic Settings > System Diagnostics** in the VMP Service Manager GUI.

The System Diagnostics table displays the available system logs:

- Name—Name of the system log (required). The name is a string of any length. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Log Label—Description of the log (required). The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
- Region—Region for which alarms are being logged (required). The default region is **0**.
- Start Time—Time the log started, or is to start. Specify the time using the following format:

  `MM/DD/YYYY HH:MM:SS`
  `Instant`
  The Start Time field uses the time zone specified in **admin > Preferences**.
- Log Duration—Time the log is to run. Specify **Indefinite** if the log is to run indefinitely, or specify the time the log is to run using the following format:

  `Number_of_days,HH:MM:SS`
  `Indefinite`
  The Log Duration field uses the time zone specified in **admin > Preferences**.
- Log Level—Level of alarm to log. Valid levels are **Info** (the default setting), **Warn**, **Minor**, **Major**, **Critical - few logs**, and **Debug**.
- State—Indicates whether the log is **Enabled** or **Disabled**.

To display the conditions associated with a log, click its **Expand** arrow. The Conditions table is displayed.

The Conditions table displays the following information:

- Application Type—Type of application for which alarms are to be logged. Drop-down types are:
  - **AWM**
  - **MCE**
  - **SM**
  - **Controller**
  - **MPE**

You can also enter any other type in the field.

- Application Function—Function of the application being logged.

  For AWM applications, drop-down functions are:

  - **Asset Lookup**
  - **Asset Management**
  - **Workflow Management**

  For MCE applications, drop-down functions are:

  - **C2Parser**
  - **Capture**
  - **CIF Generator**
  - **Indexer**
  - **Media Chunk**
  - **Storage Interface**
  - **TTML**
  - **Session Controller**

  For SM applications, drop-down functions are:

  - **Authentication**
  - **Config**
  - **HA**

  For Controller applications, drop-down functions are:

  - **SICM**

  You can also enter any other function in the field.

- Flow Type—Type of flow for which alarms are to be logged.

  For AWM applications, the drop-down type is:

  - **Content ID**

  For MCE applications, drop-down types are:

  - **Content ID**
  - **Stream Profile**

  For SM applications, there are no drop-down types.

  For Controller applications, there are no drop-down types.

  You can also enter any other type in the field.

- Flow ID—ID of the flow being logged.

- Path Type—Type of path for which alarms are to be logged.

  For AWM applications, there are no drop-down types.

  For Controller applications, there are no drop-down types.

  For MCE applications, the drop-down type is:

  – **IP Address**

  For SM applications, drop-down types are:

  – **IP Address**

  – **Source IP Address**

  You can also enter any other type in the field.

- IP Address—IP address of the path for which alarms are to be logged.

To delete a condition from a log, edit the log, then click **Delete**.

To edit a condition for a log, edit the log, then select a condition and click the **Edit**  icon to display the Edit Condition popup.

To add a condition to a log, edit the log, then click **the + button** to display the Add Condition popup.

Click the **Collapse** arrow to collapse the conditions information.

Displaying Service Diagnostics

To display service diagnostics for the VMP, select **Monitoring > Diagnostic Settings > Service Diagnostics** in the VMP Service Manager GUI.

The Service Diagnostics table displays the available system logs:

- Name—Name of the service log (required). The name is a string of any length. Acceptable characters include uppercase and lowercase letters, numbers, periods (.), dashes (-), and underscores (_). The name must not begin with a period (.), and it is not case-sensitive.
- Log Label—Description of the log (required). The description is a string of any length, and can include uppercase or lowercase letters, numbers, and any special characters.
- Service Instance—Service instance for which alarms are being logged (required).
- Start Time—Time the log started, or is to start. Specify the time using the following format:

  ```
  MM/DD/YYYY HH:MM:SS
  Instant
  ```

- Log Duration—Time the log is to run. Specify **Indefinite** if the log is to run indefinitely, or specify the time the log is to run using the following format:

  ```
  Number_of_days,HH:MM:SS
  Indefinite
  ```

- Log Level—Level of alarm to log. Valid levels are **Info** (the default setting), **Warn**, **Minor**, **Major**, **Critical - few logs**, and **Debug**.
- State—Indicates whether the log is **Enabled** or **Disabled**.

To display the conditions associated with a log, click its **Expand** arrow. The Conditions table is displayed.

The Conditions table displays the following information:

- Application Type—Type of application for which alarms are to be logged. Drop-down types are:
  - **AWM**
  - **MCE**
  - **SM**
  - **MPE**

  You can also enter any other type in the field.
- Application Function—Function of the application being logged.

  For AWM applications, drop-down functions are:
  - **Asset Lookup**
  - **Asset Management**
  - **Workflow Management**

  For MCE applications, drop-down functions are:
  - **C2Parser**
  - **Capture**
  - **CIF Generator**
  - **Indexer**
  - **Media Chunk**
  - **Storage Interface**
  - **TTML**
  - **Session Controller**

  For SM applications, drop-down functions are:
  - **Authentication**
  - **Config**
  - **HA**

  You can also enter any other function in the field.

  For Controller applications, the drop-down types are
  - **SIC**
  - **AIC**
  - **Task Controller**
  - **Service Agent**

  You can also enter any other type in the field.
- Flow Type—Type of flow for which alarms are to be logged.

For AWM applications, the drop-down type is:

- **Content ID**

For MCE applications, drop-down types are:

- **Content ID**
- **Stream Profile**

For SM applications, there are no drop-down types.

- Flow ID—ID of the flow being logged.
- Path Type—Type of path for which alarms are to be logged.

  For AWM applications, there are no drop-down types.

  For Controller applications, there are no drop-down types.

  For MCE applications, the drop-down type is:

  - **IP Address**

  For SM applications, drop-down types are:

  - **IP Address**
  - **Source IP Address**

  You can also enter any other type in the field.
- IP Address—IP address of the path for which alarms are to be logged.

To delete a condition from a log, edit the log, then click **Delete**.

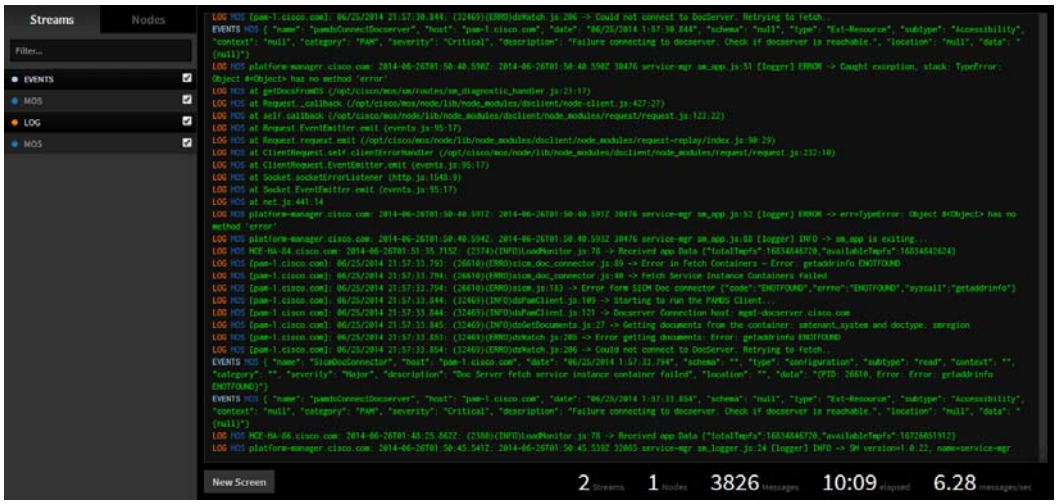
To edit a condition for a log, edit the log, then select a condition and click **Edit** to display the Edit Condition popup.

To add a condition to a log, edit the log, then click **Add Row** to display the Add Condition popup.

Click the **Collapse** arrow to collapse the conditions information.

Displaying Logs

To display logs for the VMP, select **Monitoring > Logs > Log Viewer** in the VMP Service Manager GUI. The GUI opens the VMP Log Viewer in a new tab. (The GUI actually invokes the CLS VM's log viewer.)

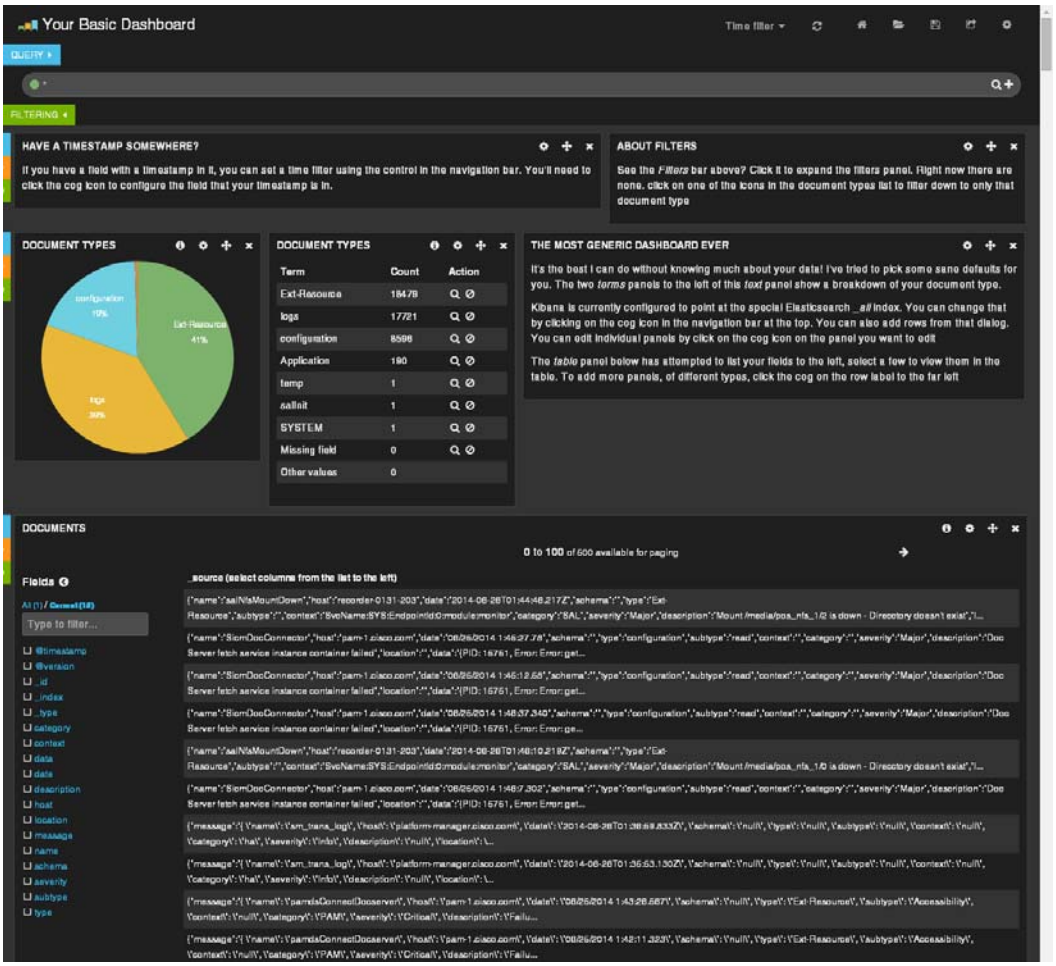


Select the **Streams** tab and the **Events** checkbox to display all of the VMP events; the **Logs** checkbox to display all of the VMP logs; or both.

Select the **Nodes** tab and the **Events** checkbox to display all of the VMP events; the **Logs** checkbox to display all of the VMP logs; or the **VMP** checkbox to display both.

Analyzing Logs

To display log analysis for the VMP, select **Monitoring > Logs > Log Analysis** in the VMP Service Manager GUI. The GUI opens the VMP Log Analysis Dashboard in a new tab.



Displaying Events

To display system and service events for the VMP, select **Monitoring > Events** in the VMP Service Manager GUI.

The GUI automatically refreshes the Event Browser table every five (5) minutes.

Select an event range for the Event Browser table:

- **Last 1 hour**
- **Last 24 hours**
- **Last 7 days**

The Event Browser table displays the following information for each event:

- Time—Time that the event occurred, in the format **DAY MONTH DATE YEAR HH:MM:SS GMT-OFFSET** (for example, **Mon Aug 04 2014 01:52:59 GMT-0700**.)
- Entity Scope—Scope of the event, such as a region or service.
- Source Node—IP address of the source node that reported the event.
- Source Image Type—Type of the source node for the event, such as **PAM**.

- Source Personality—Personality of the source node for the event, such as **Control** or **Worker**.
- Location—IP address of the location where the event occurred.
- Severity—Severity of the event: **Info**, **Warning**, **Major**, or **Critical**.
- Event Type—Type of the event, such as **Application** or **Node**.
- Event Subtype—Subtype of the event, such as **Interface** or **Health**.
- Event—Event, such as **DnsUpdate** or **ServiceInstanceUpdate**.
- Description—Description of the event.
- Events Dropped—Number of dropped events.
- Transaction ID—Indicates the specific transaction for which the alarm was generated.

Displaying Alarms

To display Active alarms for the VMP, select **Monitoring > Alarms > Active** in the VMP Service Manager GUI.

The Alarms table displays the following information for each alarm:

- Set Time—Time that the alarm occurred, in the format **DAY MONTH DATE YEAR HH:MM:SS GMT-OFFSET** (for example, **Mon Aug 04 2014 01:52:59 GMT-0700**.)
- Alarm—unique name created by the alarm source for the alarm in the format “scope-name.instance.alarmName
- Severity—Severity of the alarm
- Description—Type of alarm
- Node—IP address of the source node
- Image type—type of the source node for the alarm
- Personality—personality of the source node for the alarm
- Location—IP address of the location where the alarm occurred
- Type—Type of the alarm
- Subtype—subtype of the alarm
- Category—category may be used to identify all related alarms, for example, alarms of a particular asset workflow. It should be prefixed with application name to prevent name collision.
- Acknowledged—GUI Operator can acknowledge the alarm by selecting the alarm and clicking on the acknowledge button. This indicates that the operator has noticed the alarm.
- User—ID of the operator who acknowledged the alarm

To display History Alarms for the VMP, select **Monitoring > Alarms > History** in the VMP Service Manager GUI.

- Set Time—Time that the alarm occurred, in the format **DAY MONTH DATE YEAR HH:MM:SS GMT-OFFSET** (for example, **Mon Aug 04 2014 01:52:59 GMT-0700**.)
- Alarm—Unique name created by the alarm source for the alarm in the format “scope-name.instance.alarmName
- Cleared Time—Time at which the alarm was moved from raised/active state to cleared state, i.e. issue resolved.

- Severity—Severity of the alarm
- Description—Type of alarm
- Node—IP address of the source node
- Image type—Type of the source node for the alarm
- Personality—personality of the source node for the alarm
- Location—IP address of the location where the alarm occurred
- Type—Type of the alarm
- Subtype—Subtype of the alarm
- Category—Category may be used to identify all related alarms, for example, alarms of a particular asset work flow. It should be prefixed with the application name to prevent name collision.

Troubleshooting VMP Problems

The following sections contain information to help you troubleshoot problems when installing, deploying, configuring, and monitoring the VMP.

- Troubleshooting the VMP-M GUI, page 121
- Troubleshooting Deployment, page 122
- Troubleshooting Access/Configuration, page 122
- Troubleshooting Playback Failures, page 126
- Troubleshooting the PAM, page 136
- Troubleshooting the PAM Service Manager, page 140
- Troubleshooting the PAM DocServer, page 143
- Troubleshooting the PAM SICM, page 146
- Troubleshooting the VMP-M GUI, page 146
- Troubleshooting the MCE, page 147
- Troubleshooting the MPE, page 164
- Troubleshooting the SAL, page 169
- Troubleshooting the AWM, page 172
- Troubleshooting the Service Instances, page 182

Troubleshooting the VMP-M GUI

The VMP GUI provides valuable troubleshooting functions, including system diagnostics, service diagnostics, logging, and events. For more information, see the following sections:

- Displaying High-Level Overview Information for the VMP, page 76
- Displaying System Diagnostics, page 112
- Displaying Service Diagnostics, page 114
- Displaying Logs, page 116
- Analyzing Logs, page 117
- Displaying Events, page 118

Troubleshooting Deployment

- OVA Does Not Deploy, page 122

If this procedure does not resolve the problem, use the VMware interface to investigate.

OVA Does Not Deploy

Impact on the End User

The OVA did not deploy successfully (failed to start or did not complete).

Possible Reasons for Problem

- Bad MD5 checksum
- VM resources problem

Resolution/Logs: MD5 Checksum

Verify the posted MD5 checksum with the downloaded image.

Resolution/Logs: VM Resources

Check the VMWare logs.

Troubleshooting Access/Configuration

- VMP-M GUI Not Accessible—Network Connectivity, page 122
- VMP-M GUI Not Accessible—PAM Rebooting or Powered Off, page 123
- VMP-M GUI Not Accessible—PAM & External DNS Interaction, page 123
- Problem Logging In to VMP-M GUI, page 124
- Cannot Save Configuration In VMP-M GUI, page 124
- 500 Server Error, page 124
- 400 Bad Request or 404 Not Found, page 125

If the procedures in this section do not resolve the problem, collect the following log from the PAM:

```
tar -cvf logs.tar /var/log/*
```

VMP-M GUI Not Accessible—Network Connectivity

Impact on the End User

The VMP Manager (VMP-M) GUI is not accessible.

Possible Reasons for Problem

Network connectivity

Error/Event Messages

Examine the /var/log/tomcat/catalina.out file for error/exception messages like the following:

```
SEVERE: Exception initializing page context
java.lang.IllegalStateException: Cannot create a session after the response has been committed at
org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:102)
```

Examine the /var/log/supervisor/supervisord.log file for the following message:

```
INFO exited: docserver_app (exit status 7; not expected)
```

Resolution/Logs

1. Ping the device to see if it can be reached.
2. If the device cannot be reached, correct the networking issue.
3. If the device can be reached, log in to the PAM and verify the presence of the VMP-M GUI process status using the **supervisorctl status** command.
4. If the VMP-M GUI process is not running, examine the catalina.out logs for more details about the process failure.
5. If any of the processes are not in **RUNNING** state, use the following command to restart the process:

supervisorctl *process_name* **restart**

VMP-M GUI Not Accessible—PAM Rebooting or Powered Off

Impact on the End User

The VMP GUI is not accessible.

Possible Reasons for Problem

PAM is rebooting or powered off

Error/Event Messages

Examine the /var/log/supervisor/supervisord.log file for CRITICAL, WARNING, and ERROR error messages.

Resolution/Logs

Check the power state of the PAM VM in VCenter.

VMP-M GUI Not Accessible—PAM & External DNS Interaction

Impact on the End User

The VMP-M GUI is not accessible.

Possible Reasons for Problem

Interaction between PAM & External DNS

Error/Event Messages

Examine the /var/named/data/named.run this file for error messages.

Resolution/Logs

a. Need to make sure leadership election is proper and that the interaction with the external DNS is working properly.

b. NTP clock should be present for both PAM nodes and DNS servers.

Even after making sure the DNS interaction is fine, the log_export could be a very useful CLI which collects all required logs and can export to any ftp server. Logs could then be accessed to locate the issue.

```
 [admin@PAMx1-1 ~]$ sudo log_export
Usage: /opt/cisco/VMP/bin/log_export [-d | --delete-exported-logs] <FTP_SERVER> <USER> <PASSWORD>
```

```
Export log files under /var/log to remote FTP server.

FTP_SERVER                      FTP server hostname / IP
USER                            FTP server user name
PASSWORD                        FTP server password
[-d | --delete-exported-logs]     Delete exported log files
[--help]                        Display usage
[admin@PAMx1-1 ~]$
```

Problem Logging In to VMP-M GUI

Impact on the End User

The user cannot log in to the VMP-M GUI.

Possible Reasons for Problem

Incorrect login credentials

Error/Event Messages

If access is denied, the /var/log/tomcat/catalina.out log file provides more details about the problem. Examine the file for error messages like the following:

```
ACCESS_AUDIT_GRANTED: %[ch=wap][mid=1005]: Granted access to user admin with Authorizations
[defaultAccess] is attempting to access FilterInvocation
```

Resolution/Logs

Use the default username/password **admin**/**default**.

Cannot Save Configuration In VMP-M GUI

Impact on the End User

The user is ejected from the VMP-M GUI when trying to save the VMP configuration.

Possible Reasons for Problem

Idle timeout after one hour (60 minutes)

Error/Event Messages

The user is returned to the VMP-M GUI login screen.

Examine the var/log/tomcat/catalina.out log file for process errors.

Resolution/Logs

Make and save a configuration change, or click a tab or refresh icon, before the one-hour idle timeout expires.

If the problem persists, try to log in using a different web browser.

500 Server Error

Impact on the End User

The VMP configuration/status APIs return a 500 Server Error error code.

Possible Reasons for Problem

The PAM is powered off or rebooting

Network error

Service Manager/DocServer application error

Error/Event Messages

Examine the /var/log/supervisor/pam-restapi.err.log log file for error messages like the following:

```
error: [Errno 32] Broken pipe
```

Resolution/Logs

Verify that the PAM IP address can be reached.

Verify that all the processes are in **RUNNING** state, using the **supervisorctl status** command.

400 Bad Request or 404 Not Found

Impact on the End User

The VMP configuration/status APIs return a 400 Bad Request or 404 Not Found error code.

Possible Reasons for Problem

There is an incorrect URI or body in the API call.

Error/Event Messages

Examine the /var/log/supervisor/pam-restapi.err.log API error log file and verify that the response is 200 OK.

If the response is anything other than 200 OK, examine the /var/log/opt/cisco/VMP/errorlog/service-mgr-errorlog.current log file for error messages like the following:

```
(ERRO)sm_watcher.js:33 -> Error retrieving documents, containerId = smregion_0, objType=smdiagnostics
```

Resolution/Logs

Verify that the request contains no formatting errors, and that the attempted operation is supported. See the *Cisco Media Origination System Release API Guide* for the correct formatting.

Correct the formatting and try the API requests again.

AWM GUI Overview

- AWM GUI is running within the VMP-M GUI application which runs on top of the node server.
- The AWM GUI runs on each PAM VM and binds to port 8023 for HTTPS access (not for external)
- This GUI is accessible from the VMP-M GUI service instant context.
- The AWM GUI is started by supervisord, and is automatically restarted in case of failure.

AWM GUI Page Not Found

If you see a Page Not Found error when trying to launch the AWM GUI, take the following steps to resolve the problem.

1. Log in to the PAM VM using the VM address specified in the VMP-M GUI URL.
2. Enter the following command to determine whether the AWM GUI server is running.

```
supervisorctl status awm-ui
```

3. If the awm-ui is not running, enter the following command to start it.

```
supervisorctl restart awm-ui
```

Troubleshooting Playback Failures

- Playback Failure—DNS Problem, page 126
- Playback Failure—NTP Problem, page 127
- Playback Failure—Network Connectivity Problem, page 127
- Playback Failure—Basic Configuration Problem, page 128
- Playback Failure—Incorrect Bitrate Configuration, page 128
- Playback Failure—Captions/TTML Not Visible, page 128
- Playback Failure—Captions/TTML Out of Sync, page 128
- Playback Failure—Incorrect Symbols in Captions, page 129
- Playback Failure—ESAM Problem, page 129
- Playback Failure—Capture Unsuccessful, page 129
- Playback Failure—Service Instance Not Activated, page 130
- Playback Failure—Asset Workflow Template Not Enabled, page 130
- Playback Failure—Endpoint VIP Config Failure, page 130
- Capture Unsuccessful, page 131
- cDVR Capture Failed to Start, page 131
- Service Instance Not Activated—VM Resources, page 133
- Service Instance Not Activated—Image Version, page 133
- Bad Playback Quality—Bitrate Settings, page 133
- Bad Playback Quality—Jittery Network, page 134
- Bad Playback Quality—Jittery Feed, page 134
- Multi-Language Problems, page 134
- DVR Window Problems, page 135
- Trickmode Problems, page 135
- Variant Playlist Problems, page 135
- General Playback Failure/Buffering, page 136

Playback Failure—DNS Problem

Impact on the End User
Playback failed.

Possible Reasons for Problem
DNS problems

Error/Event Messages

Verify that the /var/log/opt/cisco/VMP/errorlog/ pam-dns-errlog.current error log file does not contain any errors.

Verify that the FQDN entry is correct for the playback callout URL.

Resolution/Logs

Verify that the client receives an appropriate redirect to the MPE-IPVS.

Verify that the MPE-IPVS provides the correct redirect information for reaching the MPE-Worker.

Verify that the DNS transaction key is valid and has not expired.

Playback Failure—NTP Problem

Impact on the End User

Playback failed.

Possible Reasons for Problem

NTP configuration or synchronization problem

Error/Event Messages

Verify that the NTP server is running and able to sync up:

Resolution/Logs

Verify that the PAM, DNS servers, MCE-Workers, MPE-Workers are all time-synchronized.

Playback Failure—Network Connectivity Problem

Impact on the End User

Playback failed.

Possible Reasons for Problem

Network connectivity problem

Error/Event Messages

Check the connectivity between the following components:

- Client and PAM
- Client and MPE
- MPE and PAM
- MPE and DRM server
- MPE and MCE
- MCE and PAM

Resolution/Logs

Verify that the client can reach the DNS server.

Verify that the client can reach the MPE-IPVS given by the DNS-server's redirect response.

Verify that the client can reach the MPE-Worker.

Playback Failure—Basic Configuration Problem

Impact on the End User

Playback failed.

Possible Reasons for Problem

Basic configuration problem

Error/Event Messages

Verify that the VMP configuration is intact. See the *Configuring the VMP Using the VMP Manager GUI, page 50*.

Resolution/Logs

Confirm that all settings are set as intended through the VMP-M GUI or API.

Playback Failure—Incorrect Bitrate Configuration

Impact on the End User

Playback failed.

Possible Reasons for Problem

Incorrect configuration of bitrates

Error/Event Messages

Enable trace error logging in the MPE:

Look for bitrate mismatch-related logs to confirm that the problem is a bad bitrate configuration.

Resolution/Logs

Verify that the bitrate settings in the Asset Publish Templates are correct. Deviations exceeding 5% of the actual stream bitrate can cause problems.

Playback Failure—Captions/TTML Not Visible

Impact on the End User

Playback failed.

Possible Reasons for Problem

Captions/TTML not visible

Resolution/Logs

Verify that the required Captions/TTML are present in the source feed.

Examine the logs in the MPE for more information about the problem.

Playback Failure—Captions/TTML Out of Sync

Impact on the End User

Playback failed.

Possible Reasons for Problem

Captions/TTML out of sync between video and audio

Problem with the client

Error/Event Messages

Look for error and event messages at the client.

Resolution/Logs

Verify that the captions/TTML are synced between the video and the audio in the original feed.

Restart the client and verify that the captions/TTML are synced between the video and the audio in the playback.

Playback Failure—Incorrect Symbols in Captions

Impact on the End User

Playback failed.

Possible Reasons for Problem

Escape sequences such as **>** instead of **>** and other symbols in captions

Error/Event Messages

Examine the client player screen for this problem

Resolution/Logs

This is a known player issue that must be addressed by the player vendor or developer.

Playback Failure—ESAM Problem

Impact on the End User

Playback failed.

Possible Reasons for Problem

ESAM advertisement not honored

Error/Event Messages

N/A

Resolution/Logs

Verify that the POIS server is up.

Verify network connectivity between the POIS server and the DCM server.

Verify network connectivity between the POIS server and the MCE-Workers.

Playback Failure—Capture Unsuccessful

Impact on the End User

Playback failed.

Possible Reasons for Problem

Capture was unsuccessful

Error/Event Messages

See the Capture Unsuccessful, page 131.

Resolution/Logs

See the Capture Unsuccessful, page 131.

Playback Failure—Service Instance Not Activated

Impact on the End User

Playback failed.

Possible Reasons for Problem

Service instance not activated successfully

Error/Event Messages

See the Service Instance Not Activated—VM Resources, page 133 and the Service Instance Not Activated—Image Version, page 133.

Resolution/Logs

See the Service Instance Not Activated—VM Resources, page 133 and the Service Instance Not Activated—Image Version, page 133.

Playback Failure—Asset Workflow Template Not Enabled

Impact on the End User

Playback failed.

Error/Event Messages

See the AWT Not Enabled—Asset Resolver Problem, page 176 and the Bad Playback Quality—Bitrate Settings, page 133.

Resolution/Logs

See the AWT Not Enabled—Asset Resolver Problem, page 176 and the Bad Playback Quality—Bitrate Settings, page 133.

Playback Failure—Endpoint VIP Config Failure

Impact on the End User

Playback failed.

Possible Reasons for Problem

Playback Endpoint VIP Config Failed

Resolution/Logs

a. zookeeper details is helpful to debug IPVS nodes details.

b. make sure VIP is assigned to IPVS nodes. If assigned, check the service agent logs to see further details about the issue.

```
[zk: localhost:2181(CONNECTED) 1] get /VMP/services/ums-0-5/apps/ums-0-5-smplaybackep-x1pe11/
ipvsConfig    ipvsNodes     status        command       state         awmConfig     workers
script        messages      handler
```

```
[zk: localhost:2181(CONNECTED) 1]
```

c. make sure external DNS server is able to resolve the request domain to the MPE-IPVS to get the MPE-Worker details, nslookup, dig are useful commands to make sure the DNS resolution happens correctly.

Capture Unsuccessful

Impact on the End User

The capture was unsuccessful.

Possible Reasons for Problem

Storage setup problem

Error/Event Messages

Verify that the cksum of the MPD update in the MCE is updating periodically:

```
cksum MPD
```

Examine the following error log in the MCE for more information about the capture failure:

```
[root@MCE-1 ~]# cd /var/log/opt/cisco/VMP/errorlog/
[root@MCE-1 errorlog]# cat service-agent-log.current | grep ERR
04/15/2014 15:08:57.612: (7089)(ERRO)MceAgent.js:205 -> Invalid SalConfig “”04/15/2014 15:54:41.498:
(7089)(ERRO)CareReceiver.js:316 -> Getting data failed
/VMP/services/live-0-3/apps/live-0-3-smcaptureep-CE1/workers/live03-smcaptureep-CE1-0/command
Exception: NO_NODE[-101]
```

Resolution/Logs

Verify that the storage is of NFS type.

Verify connectivity to the storage device.

Verify the appropriate capacity settings on the storage device.

cDVR Capture Failed to Start

Possible Reasons for Failure

The MCE Task Controller might have passed the wrong configuration:

- The ZooKeeper path is not present.
- The ZooKeeper server is not present.
- The ZooKeeper is not running
- The “instancePath” is not present.
- The “interfaces” is not present or is configured incorrectly.
- The “recordingStart” is not present or start time past the current stream time and duration.
- The “recordingDuration” is not present or configured incorrectly.
- The SourceURL/SourceIP for the profiles is not valid.
- Capture Endpoint VIP Configuration Failure

Correcting the Problem

- Check the configuration on the VMP GUI for any errors
- Disable and enable the asset work flow.
- zookeeper details could be helpful to debug HAProxy nodes details and to make sure VIP is assigned to HAProxy nodes. If assigned, check the service agent logs to see further issues.

```
[zk: localhost:2181(CONNECTED) 1] get /VMP/services/ums-0-5/apps/ums-0-5-smcaptureep-xxx
 ipvsConfig   ipvsNodes    status       command      state        awmConfig    workers
script       messages     handler
```

For more logs, customers can use log_export command to collect all the required logs and export it to any ftp server. From there support/eng team could access the logs to find out the issue.

Impact on the End User

The recording does not start.

Affected Module

cDVR Capture Application

VOD Capture Failed to Start

Possible Reasons for Failure

- The ZooKeeper server is not present.
- The ZooKeeper is not running
- The “instancePath” is not present.
- The “interfaces” is not present or is configured incorrectly.
- The sourceURL for the profiles is not valid or the file location is not accessible or the file is not present/corrupted or not a supported format.

Correcting the Problem

Check the configuration on the VMP GUI for any errors

Disable and enable the asset workflow.

Impact on the End User

The recording does not start.

Affected Module

VOD Capture Application

VOD/cDVR/LIVE Capture Failed with Storage Failure

Possible Reasons for Failure

- COS/NAS storage down or not reachable
- COS/NAS storage writes failed.
- Storage network interface down.

Correcting the Problem

Check for possible errors or alarms on external NAS storage or COS.

Check for storage usage.

Check for network connectivity between MCE nodes and COS/NAS storage.

Impact on the End User

The recording will stop and may relocate to another worker.

Also refer to cDVR Capture Failed to Start, page 131.

Service Instance Not Activated—VM Resources

Impact on the End User

The service instance failed to activate successfully.

Possible Reasons for Problem

Number of available VM resources is less than the minimum SLA

Error/Event Messages

The transaction logs show the node status of the application belonging to the affected service instance as either **critical** or **warning**. For example:

```
2014-04-17 14:10:53 SIC 10366 App Status update - vod_2_default-smcaptureep-0 critical
```

Resolution/Logs

Add the VM resources and re-enable the service instance.

Service Instance Not Activated—Image Version

Impact on the End User

The service instance failed to activate successfully.

Possible Reasons for Problem

Image version does not match the version configured in the image manifest

Error/Event Messages

In the VMP-M GUI, verify that the image version of the installed VM matches the version configured in the image manifest.

Resolution/Logs

Add new VMs with the required version, or change the version of the existing VMs and re-enable the service instance.

Bad Playback Quality—Bitrate Settings

Impact on the End User

Playback video quality is jittery or micro-blocking

Possible Reasons for Problem

Bitrate settings

Error/Event Messages

Examine the transaction logging mpe worker node. The time to serve the fragment indicates whether the network can deliver the fragment to the client with good quality.

Resolution/Logs

Check the bitrate settings in the Asset Publish Template configuration.

Bad Playback Quality—Jittery Network

Impact on the End User

Playback video quality is jittery or micro-blocking

Possible Reasons for Problem

Network is jittery

Error/Event Messages

N/A

Resolution/Logs

Check the network quality statistics, including latency, loss, and jitter.

Bad Playback Quality—Jittery Feed

Impact on the End User

Playback video quality is jittery or micro-blocking

Possible Reasons for Problem

Original feed might be jittery

Error/Event Messages

N/A

Resolution/Logs

View the original feed.

Multi-Language Problems

Impact on the End User

Multi-language does not play.

Possible Reasons for Problem

Source might be having problems sending out multi-language streams

Error/Event Messages

The MPE's transaction log shows the requests for different languages selected from the player. Look for 404/500 error codes in the response.

Resolution/Logs

Fix the source issue and try playback again.

If the issue persists, examine the MPD file generated by the MCE for the list of all available audio/video bitrate details.

In the Asset Publish Template, verify that the multiple audio bitrates are properly configured (per the source).

DVR Window Problems

Impact on the End User

The DVR window not displayed properly in the player.

Possible Reasons for Problem

DVR window configuration not pushed properly to MCE device

NFS mount point problems

Poor NFS storage device performance

Error/Event Messages

The MCE service agent logs error messages like the following:

```
[root@MCE-1 ~]# cd /var/log/opt/cisco/VMP/errorlog/
[root@MCE-1 errorlog]# cat service-agent-log.current | grep ERR
04/15/2014 15:08:57.612: (7089)(ERRO)MceAgent.js:205 -> Invalid SalConfig “”
```

Trickmode Problems

Impact on the End User

Trickmode does not work correctly.

Possible Reasons for Problem

DVR window configuration is incorrect

Performance problems with NFS read/write access

Error/Event Messages

Examine the MPE’s transaction logs for 404/500 error codes in the fragment responses.

Resolution/Logs

Verify that the DVR window configuration is correct and the NFS performance is good.

Variant Playlist Problems

Impact on the End User

The variant playlist is not rendered to the clients

Possible Reasons for Problem

Variant bitrate configuration (video/audio) incorrect

Error/Event Messages

Examine the MPE’s transaction logs for 404 error codes.

Resolution/Logs

Verify that the variant video and audio bitrates are configured correctly (per the source, and within the 5% buffer limit).

General Playback Failure/Buffering

Impact on the End User

There are general playback failures and buffering problems.

Possible Reasons for Problem

For Live playout, HTTP header policies configured incorrectly

Error/Event Messages

Examine the MPE's transaction logs for 404 error codes that indicate that the header policy is not defined correctly for Live playout.

Error/Event Messages

For Live playout, verify that the manifest expiry header and the cache-control header value are set to zero (0).

Player on buffering mode/404 Error on MCE/MPE During Redundancy Test.

Problem/Impact

There is a small window when the MCE goes down and is detected an updated to all MCEs during which a request is initiated from the client, a 502 error occurs.

Possible Reasons for Problem

During the time that one MCE goes down, it takes approximately 8 seconds before requests can be handled. Based on current behavior and design, this is expected.

Resoulution

Player needs a refresh.

Troubleshooting the PAM

The following sections contain information to help you troubleshoot problems involving the PAM.

- Verifying That All Processes Are Running on a PAM HA Node, page 136
- Installed VM Not Found, page 137
- Rest API (DNS) Returns 500 Internal Server Error, page 137
- Rest API (DNS) Returns 500 Internal Server Error, or Process Not Coming Up, page 137
- Reboot of ZooKeeper Leader Node Returns 500 Internal Server Error, page 139
- When Using the External DNS, nslookup Is Not Working From the PAM, page 139
- PAM Cannot Update the DNS Entry in the External DNS, page 139
- Redis AppEngine Node Failure, page 140

Verifying That All Processes Are Running on a PAM HA Node

To verify that all processes are running on a PAM HA node, issue the following API call:

```
GET http:pam_node:5067/v1/roles/leaders
```

Verify that the response includes the following roles:

```
[rabbitmq, pam-installedVm, pam-docserver, cos-controller, pam-dns, service-mgr, pam-platsrv, pam-zone,
controller, pam-vmLoadBalancer, mgmt-docserver, mongo]
```

Installed VM Not Found

When nodes are added to the VMP-M GUI, an AIC requesting the VM might return a “VM not found” error.

If this error is returned, take the following steps to diagnose the problem:

1. Check the /var/log/opt/cisco/VMP/errorlog/pam-docserver-errorlog.current file.

The cli_pamds-errorlog.current file should contain the node name that was configured and the REST API to the PAM. Look for the REST API response.

- If the REST API response is not present, the pam-docserver has not yet received the watch from the DocServer.
- If the response is present, check the response code. If the code is 400 Bad Request, some of the parameters in the node object might not have passed validation.

2. Check the /var/log/opt/cisco/VMP/errorlog/pam-installedVm-errorlog.current file.

Look for the **update** keyword along with the name of the node. You might see one of the following errors in the logs:

- Interface type not found—A mandatory interface was not provided for the node.
- IP not reachable—The PAM cannot reach the Management interface IP address.
- Interface must be an address—There is a misspelling or other typographical error in the interface field for the node.
- Duplicate IP exists—One of the nodes is using the same IP address as this interface.
- Zone needed for VM—The zone field, which is mandatory for an installed VM, is missing.
- Zone not found—The zone field that was entered is not configured.
- Image Personality needed for VM—The image personality, which is mandatory for the VM, is missing.

Rest API (DNS) Returns 500 Internal Server Error

A REST API call to add a record to the DNS might return a 500 Internal Server Error.

If this error code is returned, one of the following problems might have occurred:

- The DNS process might not have been initialized, resulting in a timeout for the REST API call. Look in the /var/log/opt/cisco/VMP/errorlog/pam-dns-errorlog.current file to see if the REST API call reached the DNS process.
- The DNS process might have crashed. If so, the /var/log/supervisor/pam-*process name*.err.log file shows the error exception.

Rest API (DNS) Returns 500 Internal Server Error, or Process Not Coming Up

A REST API call to add a record to the DNS might return a 500 Internal Server Error.

If this error code is returned, the process might not be up, or a leader might not have been elected for the process. Use the following procedure to analyze the problem:

1. Run **zkCli.sh** and use **ls /roles** to examine the corresponding node.

If the node is present, use **ls /role/leader** to determine whether an entry in /roles has a corresponding entry in /role/leader. If that is the case, that process might be crashing repeatedly.

2. The following table maps the supervisor process name to the ZooKeeper node and associated log files.

Table 0-1

Supervisor Process	ZooKeeper Node Name	Error Log (/var/log/opt/cisco/VMP/errorlog/)	Supervisor Logs (/var/log/supervisor)	Transaction Logs /var/log/opt/cisco/VMP/translogs
pam-installedVm	pam-installedVm	pam-installedVm-errorlog.current	pam-installedVm.log pam-installedVm.err.log	pam-installedVm.log
pam-dns	pam-dns	pam-dns-errorlog.current	pam-dns.log pam-dns.err.log	pam-dns.log
pam-mongoWatch	mongo	pam-mongoWatch-errorlog.current	pam-mongoWatch.log pam-mongoWatch.err.log	mongo.log
pam-docserver	pam-docserver	pam-docserver.log	pam-docserver.log pam-docserver.err.log	pam-docserver.log
pam-platsrv	pam-platsrv	pam-platsrv-errorlog.current	pam-platsrv.log pam-platsrv.err.log	pam-platsrv.log
pam-rabbitMqWatch	rabbitmq	pam-rabbitMqWatch-errorlog.current	pam-rabbitMqWatch.log pam-rabbitMqWatch.err.log	rabbitmq.log
pam-vmLoadBalancer	pam-vmLoadBalancer	pam-vmLoadBalancer-errorlog.current	pam-vmLoadBalancer.log pam-vmLoadBalancer.err.log	pam-vmLoadBalancer.log
pam-restapi		pam-restapi-errorlog.current	pam-restapi.log pam-restapi.err.log	pam-restapi.log
pam-zone_app	pam-zone	pam-zone-errorlog.current	pam-zone.log pam-zone.err.log	pam-zone.log
mgmt-docserver	mgmt-docserver	mgmt-docserver-errorlog.current	docserver_app.log docserver_app.err.log	mgmt-docserver.log
controller	controller	VMPController-errorlog.current	VMP_launcher.log VMP_launcher.err.log	controller.log
cos-controller	cos-controller	COSController-errorlog.current	cos-aic.log cos-aic.err.log	cos-controller.log

Table 0-1

Supervisor Process	ZooKeeper Node Name	Error Log (/var/log/opt/cisco/VMP/errorlog/)	Supervisor Logs (/var/log/supervisor)	Transaction Logs /var/log/opt/cisco/VMP/translogs
service-mgr	service-mgr	service-mgr-errorlog.current	sm_app.log sm_app.err.log	sm
event-aggregator	event-aggregator	event-aggregator.current	event_aggregator.log event_aggregator.err.log	event-aggregator
roleserver	roleserver	roleserver-errorlog.current	roleserver_app.log roleserver_app.err.log	roleserver

Examine the relevant /var/log/opt/cisco/VMP/errorlog/*processName*.current logs to determine whether the Rest API call reached the corresponding process.

3. A 500 internal error can also be returned if the process crashed. Examine the /var/log/supervisor/*cli_process*.err.log to determine the exception of the error.

Reboot of ZooKeeper Leader Node Returns 500 Internal Server Error

If the ZooKeeper leader node is rebooted, a new ZooKeeper leader is elected, which can take up to 15 seconds. After the election of the new ZooKeeper leader, the other applications come up and elect their leaders. Therefore, you might see a 500 internal server error while the applications elect their leaders. This is expected behavior.

When Using the External DNS, nslookup Is Not Working From the PAM

If nslookup for the hostname.domain is not returning the desired IP address, check the external DNS for error indications.

PAM Cannot Update the DNS Entry in the External DNS

If the PAM cannot update the DNS entry in the external DNS, check the /var/log/opt/cisco/VMP/errorlog/pam-dns-errorlog.current file to determine the problem.

- If the file indicates “bad time” error, then there is a significant time difference between the PAM and the external DNS.

  To correct the problem, sync up the time between the PAM and the external DNS, or use the same NTP server for both.

- If the file indicates a “bad transaction key” error, then the transaction key might be expired or no longer valid.

  To correct the problem, regenerate the transaction key, update the external DNS to reflect the new key, and redeploy the PAM using the new key.

- If the file indicates a “bad request” error, then one or more field values might be missing or incorrect.

  To correct the problem, correct the bad field values.

Redis AppEngine Node Failure

Condition: After rebooting master redis, redis appengine is released with a fault state (service config failed). To correct the problem, follow the steps below:

- Clear the alarm by moving the node to maintenance mode and then back to In Service.
- Log into the AppEngine node and restart the Service Agent.

Troubleshooting the PAM Service Manager

- SM Overview, page 140
- SM Logging, page 140
- 400 Bad Request, Invalid JSON body sent in the request, page 141
- 400 Bad Request, Invalid JSON schema, page 141
- Bad Request, Non supported type in requestkeyprofile, page 141
- 400 Bad Request, Non supported operation for this object serviceinstances, page 142
- 400 Bad Request, Non supported type in requestserviceinstance, page 142
- 500 Internal Server Error SM internal error, owner not defined, page 143
- 503 Service Unavailable Error, page 143

SM Overview

The SM provides an interface service to manage the configuration data and monitor vital activities in the VMP. The SM binds to port 8443 for external HTTPS access, and to port 8001 for local HTTP access via loopback address (127.0.0.1).

The SM runs on a PAM VM and supports an active/hot-standby HA model. There can be multiple hot-standby SM instances, with one selected as the leader to service the API. All hot-standby SM instances complete the startup sequence, except any interface request is rejected with HTTP error 503. The leader binds to the SM FQDN via DNS. The SM FQDN has the following format:

`service-mgr.`*`domain_name`*

where:

- **service-mgr** is fixed.
- *domain_name* is derived from the OVA configuration, such as **myvideo.com**.

The SM is started by supervisord, and is automatically restarted in case of failure.

SM Logging

The VMP provides transactional logging for the PAM Service Manager.

The log messages provide the following information:

- Date
- Name and version of the application
- Remote client IP address and port number

- Full URL of the request
- Type of operation (GET, POST, PUT, DELETE)
- Request body for POST and PUT operations
- Any log messages

You can view the log messages on the VM in the /var/log/opt/cisco/VMP/errorlog directory.

The following is a sample log message for INFO:

```
[2014-02-26 15:27:08.426] [INFO] [default] -
{"date":"2014-02-26T23:27:08.425Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/serviceinstances/cos_0_default/asset
workflowtemplates/a123","requestBody":{"name":"0","properties":{"captureEndpointRef":"smserviceinstance
_live-0-default.smcaptureep.0","assetLifecyclePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"s
mtenant_system.smnasstore.S1","state":"Enabled"}},"message":"Creation of object assetworkflowtemplates
with Object Id a123 received"}
```

400 Bad Request, Invalid JSON body sent in the request

A REST API call might return a 400 Bad Request, Invalid JSON body sent in the request, with a log message like the following sample:

```
{"date":"2014-02-26T23:34:05.218Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/serviceinstances/cos_0_default/asset
workflowtemplates/a123","requestBody":{},"message":"Invalid JSON body sent in the request as no
properties specified"}
```

If you receive this error code, check the Content-Type in the request and make sure that it is set to **application/json**. Do not set the Content-Type to anything else. If you do so, the VMP parses the body of the request as empty properties and returns this error code.

400 Bad Request, Invalid JSON schema

A REST API call might return a 400 Bad Request, Invalid JSON schema, with the following response output:

```
SyntaxError: Unexpected string
    at Object.parse (native)
    at /opt/cisco/service-mgr/node_modules/express/node_modules/connect/lib/middleware/json.js:75:25
    at IncomingMessage.onEnd
(/opt/cisco/service-mgr/node_modules/express/node_modules/connect/node_modules/raw-body/index.js:109:7)
    at IncomingMessage.g (events.js:175:14)
    at IncomingMessage.EventEmitter.emit (events.js:92:17)
    at _stream_readable.js:920:16
    at process._tickCallback (node.js:415:13)
```

If you receive this error code, check the request body to see if any quotation marks (“) or commas (,) are missing, and verify the rest of the schema.

Bad Request, Non supported type in requestkeyprofile

A REST API call might return a 400 Bad Request, Non supported type in requestkeyprofile, with log messages like the following sample:

```
[2014-02-27 11:52:55.120] [INFO] [default] -
{"date":"2014-02-27T19:52:55.120Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/keyprofile/123","requestBody":{"name
```

":"0","properties":{"captureEndpointRef":"smserviceinstance_live-0-default.smcaptureep.0","assetLifecyc
lePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"smtenant_system.smnasstore.S1","state":"Enabl
ed"}},"message":"Creation of object keyprofile with Object Id 123 received"}
[2014-02-27 11:52:55.121] [ERROR] [default] -
**{"date":"2014-02-27T19:52:55.121Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/keyprofile/123","requestBody":{"name
":"0","properties":{"captureEndpointRef":"smserviceinstance_live-0-default.smcaptureep.0","assetLifecyc
lePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"smtenant_system.smnasstore.S1","state":"Enabl
ed"}},"message":"Bad Request, Invalid Object Type keyprofile"}**

This problem can occur if there is an invalid object name in the URL. Verify the URL and the object name sent in the URL.

400 Bad Request, Invalid URL

A REST API call might return a 400 Bad Request, Invalid URL.

If this error code is returned, verify the URL.

400 Bad Request, Non supported operation for this object serviceinstances

A REST API call might return a 400 Bad Request, Non supported operation for this object serviceinstances, with log messages like the following sample:

[2014-02-27 11:57:54.781] [INFO] [default] -
{"date":"2014-02-27T19:57:54.780Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/serviceinstances/vod_1_default","req
uestBody":{"name":"0","properties":{"captureEndpointRef":"smserviceinstance_live-0-default.smcaptureep.
0","assetLifecyclePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"smtenant_system.smnasstore.S1
","state":"Enabled"}},"message":"Creation of object serviceinstances with Object Id vod_1_default
received"}
[2014-02-27 11:57:54.781] [ERROR] [default] - [The operation create cannot be performed on the object smserviceinstance as it is not supported']
**[2014-02-27 11:57:54.781] [ERROR] [default] -
{"date":"2014-02-27T19:57:54.781Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/serviceinstances/vod_1_default","req
uestBody":{"name":"0","properties":{"captureEndpointRef":"smserviceinstance_live-0-default.smcaptureep.
0","assetLifecyclePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"smtenant_system.smnasstore.S1
","state":"Enabled"}},"message":"The operation create cannot be performed on the object
serviceinstances as it is not supported"}**

This problem indicates that an incorrect operation was performed on the object.

400 Bad Request, Non supported type in requestserviceinstance

A REST API call might return a 400 Bad Request, Non supported type in requestserviceinstance, with log messages like the following sample:

[2014-02-27 12:13:58.532] [INFO] [default] -
{"date":"2014-02-27T20:13:58.532Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/serviceinstance/vod_1_default/captur
eendpoints/cap_ep1","requestBody":{"name":"0","properties":{"captureEndpointRef":"smserviceinstance_liv
e-0-default.smcaptureep.0","assetLifecyclePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"smten
ant_system.smnasstore.S1","state":"Enabled"}},"message":"Creation of object captureendpoints with
Object Id cap_ep1 received"}
**[2014-02-27 12:13:58.533] [ERROR] [default] -
{"date":"2014-02-27T20:13:58.533Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/serviceinstance/vod_1_default/captur
eendpoints/cap_ep1","requestBody":{"name":"0","properties":{"captureEndpointRef":"smserviceinstance_liv
e-0-default.smcaptureep.0","assetLifecyclePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"smten
ant_system.smnasstore.S1","state":"Enabled"}},"message":"Bad Request, Non supported Type in request
serviceinstance"}**

This problem indicates that an incorrect parent type sent for the object in the request. Verify the parent type.

500 Internal Server Error SM internal error, owner not defined

A REST API call might return a 500 Internal Server Error SM internal error, owner not defined, with log messages like the following sample:

```
[2014-02-27 12:08:07.242] [INFO] [default] -
{"date":"2014-02-27T20:08:07.242Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/serviceinstances/vod_3_default/captu
reendpoints/cap_ep1","requestBody":{"name":"0","properties":{"captureEndpointRef":"smserviceinstance_li
ve-0-default.smcaptureep.0","assetLifecyclePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"smte
nant_system.smnasstore.S1","state":"Enabled"}},"message":"Creation of object captureendpoints with
Object Id cap_ep1 received"}
[2014-02-27 12:08:07.243] [DEBUG] [default] - [ 'smserviceinstance : smtenant' ]
[2014-02-27 12:08:07.265] [ERROR] [default] - [ 'Doc client internal error: Error: 404' ]
[2014-02-27 12:08:07.265] [ERROR] [default] -
{"date":"2014-02-27T20:08:07.265Z","appName":"service-mgr","appVersion":"1.0.17","operation":"create","
remoteClientIp":"127.0.0.1","requestUrl":"http://localhost:3000/v2/serviceinstances/vod_3_default/captu
reendpoints/cap_ep1","requestBody":{"name":"0","properties":{"captureEndpointRef":"smserviceinstance_li
ve-0-default.smcaptureep.0","assetLifecyclePolicyRef":"454545","mediaSourceRef":"ud","storageRef":"smte
nant_system.smnasstore.S1","state":"Enabled"}},"message":"owner is not defined, Error: 404"}
```

This problem indicates that containers and documents were not preloaded in the MongoDB. Verify that the necessary containers and documents were preloaded.

503 Service Unavailable Error

When trying to create a statecache endpoint, using POST Request PAM, the PAM responds with a 503 service unavailable error, with log messages like the following:

```
[root@control-pam1-staging errorlog]# showstatus .. status check running.
.............................
network: status Ok, performance n/a, execution time 32 ms
supervisord: status Failed, performance n/a, execution time 47 ms
   ... test: checking supervisord service => (45 ms) ok, service not running
   ... test: checking server ports [9001] => (4 ms) ok
   ... test: checking non running services => (146 ms) 0 supervisord processes running:!
```

If this problem persists,

- run “showstatus” on the PAM node to make sure everything is okay.
- run “supervisorctl to view the status of all processes and check to see if all is okay. If some or all processes are not coming up, try restarting the process(es).
- If that still fails, reboot or contact Technical Support.

Troubleshooting the PAM DocServer

- DocServer Overview, page 144
- DocServer Logs, page 144
- Dependency Timed Out, page 144
- DNS Update Error, page 144

- ZooKeeper Error, page 145
- DocServer Health Check, page 145

DocServer Overview

The DocServer provides a database API to store and retrieve configuration and runtime data from the MongoDB. It also provides a watcher function, notifying other applications when there are changes to the stored configuration objects.

The DocServer binds to port 5087 for interface access. Access to the database API and watcher function are provided for VMP applications indirectly through a Docclient library module. The Docclient library communicates with the DocServer via the DocServer FQDN.

The DocServer supports an active/standby HA model. There can be multiple standby DocServer instances, with one leader elected to provide the interface service. The DocServer uses RoleWatch to elect a leader at startup. The MongoDB is a prerequisite for electing a DocServer leader.

The IP address of the elected DocServer leader binds to the DocServer FQDN via DNS. The DocServer FQDN has the following format:

`mgmt-docserver.`*`domain_name`*

where:

- **mgmt-docserver** is fixed.
- *domain_name* is derived from the OVA configuration, such as **myvideo.com**.

The DocServer is started by supervisord, and is automatically restarted in case of failure.

DocServer Logs

The DocServer logs are located under /var/log/opt/cisco/VMP/errorlog/mgmt-docserver-errorlog.*.

The VMPt current log is in the /var/log/opt/cisco/VMP/errorlog/mgmt-docserver-errorlog.current file.

Dependency Timed Out

You might see the following entry in the mgmt-docserver logs:

```
... RoleWatch: checkwaitTimeout: Timed out waiting for dependencies.
```

This can occur at startup and might indicate issues with the DocServer's dependencies, if they are the only logs you see in mgmt-docserver. The DocServer is waiting for the cli_VMPdns_app and mongodocserver processes to register with ZooKeeper before starting up. If the two processes do not come up, the DocServer continues to wait indefinitely, periodically logging this entry.

If you see entries like these at the end of the DocServer logs, and you are experiencing issues with DocServer not responding, you must determine whether the two processes are up or down.

DNS Update Error

The DocServer depends on the cli_VMPdns_app to update itself for its leadership election. The following log entries indicate an error while updating the DNS process:

```
04/29/2014 18:06:19.452: (3270)(INFO)dnshelper.js:56 -> DNS uri:
http://172.22.116.86:5000/v1/VMPDns/record
```

```
04/29/2014 18:06:19.452: (3270)(INFO)dnshelper.js:67 -> updateDns: DNS Request Body:
{"domain":"cos.cisco.com","host":"pm-172-22-116-86-VMP","record":"CNAME","cname":"mgmt-docserver"},
start date = Tue Apr 29 2014 18:06:19 GMT-0400 (EDT)
04/29/2014 18:06:19.594: (3270)(DETL)dnshelper.js:87 -> updateDns: error updating dns entries... err =
null
04/29/2014 18:06:19.595: (3270)(DETL)dnshelper.js:88 -> updateDns: Total time for request = 142 msec
04/29/2014 18:06:19.596: (3270)(DETL)dnshelper.js:90 -> updateDns: error response code = 500
04/29/2014 18:06:19.597: (3270)(DETL)dnshelper.js:22 -> updateDnsWithRetry: update dns with retry left
= 0, failed with error: {"error":"response code: 500"}
04/29/2014 18:06:19.598: (3270)(INFO)rolewatch.js:306 -> Error updating DNS entries...
```

If you see the “Error updating DNS entries” message, verify that the cli_VMPdns_app is running properly.

ZooKeeper Error

The DocServer depends on the ZooKeeper to register itself for leadership, member election, and so on. If ZooKeeper issues arise, the DocServer receives an error and must restart. The following log entries indicate that the DocServer has lost its connection to the ZooKeeper:

```
04/25/2014 23:29:12.307: (4627)(TRCE)rologger.js:43 -> Disconnected from ZooKeeper.
04/25/2014 23:29:12.308: (4627)(TRCE)rologger.js:43 -> run: Client got disconnected from ZooKeeper...
waiting for 8000 msec for connect event...
04/25/2014 23:29:20.313: (4627)(INFO)rologger.js:35 -> Client connection is lost...
04/25/2014 23:29:23.362: (4627)(TRCE)rologger.js:43 -> Disconnected from ZooKeeper.
04/25/2014 23:29:23.363: (4627)(TRCE)rologger.js:43 -> run: Client got disconnected from ZooKeeper...
waiting for 8000 msec for connect event...
```

If this entry occurs after a DocServer restart and repeats in the log, there is an issue with the ZooKeeper.

DocServer Health Check

When checking the DocServer, you must not only determine that the DocServer is up, you must also determine that the processes on which the DocServer depends are up. To verify that the required processes are up and running on the node, use the following procedure:

- Enter the **ps -aef | grep zookeeper** command and verify that there is a ZooKeeper running.
- Enter the **ps -aef | grep mongod** command and verify that there is a MongoDB running.
- Enter the **ps -aef | grep redis** command and verify that there is a Redis server running.
- Enter the **supervisorctl status docserver_app** command to check the DocServer process.
- Enter the **supervisorctl status cli_VMPdns_app** to check the cli_VMPdns_app.

If there are multiple nodes, enter these commands on each node.

- DocServer Leadership Dependency, page 145
- MongoDB Sanity Check, page 146

DocServer Leadership Dependency

At startup, both the MongoDB and the cli_VMPdns_app must have a leader elected in the ZooKeeper. If either leader is absent, the DocServer hangs until both the MongoDB and the cli_VMPdns_app have leaders. Therefore, after verifying that the ZooKeeper, MongoDB, and Redis server are running, you must determine whether MongoDB and the cli_VMPdns_app have leaders. To do so, issue the following API call:

```
GET http:a="" host:5067/v1/roles/leaders
```

Verify that the response from the ZooKeeper includes all of the leaders.

If you encounter problems with the request, enter the **supervisorctl status** command to verify that the roleserver_app is up and running on the PAM node. Restart the roleserver_app, if necessary. Verify that the response contains the following entries, with valid host addresses:

```
"dns": {
    "host": "172.19.21.219",
    "port": "5000"
    }

"mongo": {
    "host": "172.19.21.219",
    "port": "5000"
    }
```

If the JSON body is empty, the leaders have not been elected. Refer to the DNS and MongoDB troubleshooting to determine why the leaders are absent.

MongoDB Sanity Check

You should perform a sanity check on the MongoDB periodically to verify that it is working properly, even if all of its processes are up and running. To do so, use the following procedure:

1. Enter the **mongo** command from the local shell.

The command prompt should change to ...PRIMARY or ...SECONDARY. If the command prompt does not change, there is a problem with the MongoDB.

2. Enter the **rs.conf()** command from the local shell and verify that all of the configured MongoDB members are present.

Troubleshooting the PAM SICM

In an HA environment, the SICMs are started by supervisord on all PAM HA nodes.

The SICMs running on the PAM HA nodes use RoleWatch to elect a leader. The DocServer is a prerequisite for electing an SICM leader.

The SICM leader queries the DocServer for all active services, and spawns SICs.

Troubleshooting the VMP-M GUI

- VMP-M GUI Overview, page 146
- VMP-M GUI Page Not Found, page 147

VMP-M GUI Overview

The VMP configuration management is provided through a browser-based GUI application, which runs on top of the Apache Tomcat. The GUI runs on each PAM VM and binds to port 8443 for HTTPS access. One of the GUI application instances is selected as the leader to provide the configuration service. The GUI leader is accessible externally through DNS resolution. The FQDN for GUI has the following format:

`ui.`*`domain_name`*

where:

- **ui** is fixed.

- *domain_name* is derived from the OVA configuration, such as **myvideo.com**.

The Tomcat is started by supervisord, and is automatically restarted in case of failure.

VMP-M GUI Page Not Found

If you see a “Page Not Found” error when trying to launch the VMP-M GUI, take the following steps to resolve the problem:

1. Log in to the PAM VM using the VM address specified in the VMP-M GUI URL.
2. Enter the following command to determine whether the Apache Tomcat server is running:

```
sudo service tomcat status
```

3. If the Tomcat is not running, enter the following command to start it:

```
sudo service tomcat restart
```

For additional troubleshooting, examine the GUI Tomcat server logs in the /usr/share/tomcat/logs/catalina.out directory.

Troubleshooting the MCE

The following sections contain information to help you troubleshoot problems involving the MCE.

- Configuration Problems, page 147
- Ingest Problems, page 148
- MCE Troubleshooting Tools, page 158

Configuration Problems

- live/cDVRCaptureSessionController failed to start, page 147
- TS Bitrate Profiles Merge to the same Profile in the MPD of MCE and M3U8 of the MPE, page 148

live/cDVRCaptureSessionController failed to start

Possible Reasons for Failure

The MPE might have received the wrong configuration:

- The ZooKeeper path is not present.
- The ZooKeeper server is not present.
- The ZooKeeper did not start.
- The “instancePath” is not present.
- The “interfaces” is not present or is configured incorrectly.
- The “tstvWindow” is not present or is set to a bad value (less than 30).
- The SourceURL for the profiles is not valid.

Correcting the Problem

Check and restart the ZooKeeper on the PAM, if needed.

Impact on the End User

The recording does not start.

Affected Module

Live/cDVR Capture Application

TS Bitrate Profiles Merge to the same Profile in the MPD of MCE and M3U8 of the MPE

Possible Reasons for Problem

Incorrect TS bitrate value configured on the DCM.

Correcting the Problem

Make sure The TS bitrate value is correct and different for every video profile.

Affected Module

DCM, MCE, MPE

Ingest Problems

- Live/cDVR Channel stops right after starting due to no EBP in the input feeds, page 149
- Input transport stream has no IDRs for H264 video, page 149
- Input transport stream is not CBR (bit-rate calculation failure), page 149
- Audio/video codec types in the input transport stream are not supported, page 149
- Input stream received empty packets (no useful data), page 150
- Packet Loss on the Input Feeds, page 150
- No Data In the Feed–Ingest Network Cannot Be Reached, page 150
- No Data In the Feed–No Data From Source Feed, page 151
- No PAT In the Feed, page 151
- No PMT In the Feed, page 152
- PTS Discontinuity, page 153
- No Audio PID In a Feed, page 154
- Same Bitrate on Two Different Profiles, page 154
- Different Profiles Have Different Audio Codecs, page 155
- Profiles In a Channel Are From Different Source Channels, page 155
- Feed is a VBR Feed, page 156
- PTS Discontinuity in the Feed, page 157
- VOD Injest-Recording Status Fails with one Failed Profile, page 157
- MCE Fail to Capture When the Feed is Changed to 25fps, page 157

Live/cDVR Channel stops right after starting due to no EBP in the input feeds

Possible Reasons for Failure

The feed is configured without EBP on the transcoder.

Correcting the Problem

On the transcoder, check the configuration of all of the feeds for the channel and verify that each of the feed is configured with EBP.

Impact on the End User

The Live/cDVR channel fails to start.

Affected Module

MCE

Input transport stream has no IDRs for H264 video

Possible Reasons for Failure

The transcoder configuration is incorrect.

Correcting the Problem

On the transcoder, check the configuration of all of the feeds for the channel and verify that each of the feed is configured with IDR.

Impact on the End User

The Live/cDVR channel stops right after starting. It fails after detecting that there is no IDP on the feeds.

Affected Module

MCE

Input transport stream is not CBR (bit-rate calculation failure)

Possible Reasons for Failure

The transcoder configuration is incorrect.

Correcting the Problem

Stop the recording for the affected profile.

Remove the recording from the MPD.

Impact on the End User

The affected profile is not available for the playback.

Affected Module

Indexer

Audio/video codec types in the input transport stream are not supported

Possible Reasons for Failure

The transcoder configuration is incorrect.

Correcting the Problem

On the transcoder, examine the configuration of the feeds and verify that the audio for all of the profiles (feeds) comes from the same codec.

Impact on the End User

HLS playback works normally, but HSS playback fails, as there is no audio fragment timeline in the MPD file.

Affected Module

MCE

Input stream received empty packets (no useful data)

Possible Reasons for Failure

The transcoder stops sending out data on the profiles.

The ingest network is down.

Correcting the Problem

Check the transcoder to make sure it is sending data to the defined multicast IP address and port.

Verify that the ingest network is up and that the MCE can receive the data from the feeds.

Impact on the End User

The Live/cDVR channel stops when there is no data coming in.

Affected Module

MCE

Packet Loss on the Input Feeds

Possible Reasons for Failure

A network issue could be causing the packet loss.

The input feeds have the packet loss.

Correcting the Problem

Check the network.

Check the input feeds from the transcoder.

Impact on the End User

The Live/cDVR channel is still running, but there might be some streaming issues on playback, such as jitters, micro-blocking, frozen, and so on.

Affected Module

MCE

No Data In the Feed—Ingest Network Cannot Be Reached

Possible Reasons for Failure

The Ingest network cannot be reached.

The source feeds are not sending any data.

The transcoder/encoder is down.

The channel is down.

Impact on the End User

There is no data in the feed on any profile.

The MPD is no longer updating.

The Live/cDVR channel stops after several minutes.

Error/Event Messages

```
04/16/2014 20:42:23.225: node(24307)ERRO:ICaptureSession.h:45-> IOM: [Read timeout occurred. Closing
session]
04/16/2014 20:42:23.226: node(24307)ERRO:Live/cDVRCaptureSession.cpp:428-> No more data on ingest
interface. Failing CaptureSession
04/16/2014 20:42:23.228: node(24307)ERRO:Live/cDVRCaptureSession.cpp:215-> Received index data of size
1476, offset 0
04/16/2014 20:42:23.228: node(24307)ERRO:indexer.cpp:410->
04/16/2014 20:42:23.228: node(24307)ERRO:indexer.cpp:411-> CIndexer: Problems during ingest!!!!
04/16/2014 20:42:23.228: node(24307)ERRO:indexer.cpp:431-> CIndexer: 3 Packets with Bad CCs
04/16/2014 20:42:23.228: node(24307)ERRO:indexer.cpp:493->
04/16/2014 20:42:23.330: node(24307)ERRO:C2ToDashIndexData.cpp:119->
~C2ToDashIndexData():119: ERROR: Failed to receive AVC-I-Picture or Audio or Gap Tag for last EBP
Record:
C2IndexRecord(EBP) Length(15)
Flags:88
SapType:251
GroupingID:2
Time: 7307491111562289224
SegmentIndex: 32245880
```

No Data In the Feed—No Data From Source Feed

Possible Reasons for Failure

The source feed is not sending any data.

There is a bad configuration on the transcoder/encoder for the affected profile.

Impact on the End User

There is no data in the feed on one of the profiles.

The MPD is no longer updating.

The playback has stopped.

Error/Event Messages

No error messages are sent to the Live/cDVRCaptureApp and live/cDVRSessionController logs.

Examine the LookupService log for error messages like the following:

```
(ERRO)LookupTable.js:21 -> Lookup failed with error: null for Channel: abc-10p1
```

No PAT In the Feed

Possible Reasons for Failure

There is a bad configuration on the transcoder/encoder for the affected profile.

The source feed to the transcoder failed.

Impact on the End User

There is no PAT in the feed.

The Live/cDVR channel failed to start.

The Live/cDVRCaptureApp and Live/cDVRSessionController started to run but then stopped immediately.

All of the resources for the affected channel were cleaned up.

Error/Event Messages

Examine the Live/cDVRCaptureApp log for error messages like the following:

```
04/21/2014 17:03:55.800: node(29377)ERRO:TrickAll.cpp:2417-> ERROR: PAT not found
04/21/2014 17:03:55.800: node(29377)ERRO:TrickAll.cpp:3075-> ERROR: No PAT found
04/21/2014 17:03:55.808: node(29377)ERRO:TrickAll.cpp:4347-> ERROR: TrickAll::ProcessMpegData Ingest
fails. Check ingest stream and/or adjust Ingest Knobs
04/21/2014 17:03:55.808: node(29377)ERRO:indexer.cpp:244-> ***CIndexer: ERROR: ProcessMpegData failed
due to bad input data msa_status 0***
04/21/2014 17:03:55.809: node(29377)ERRO:Live/cDVRCaptureSession.cpp:298-> Stopping
Live/cDVRCaptureSession because of bad input data
04/21/2014 17:03:55.810: node(29377)ERRO:TrickAll.cpp:1361-> ERROR: TrickAll::Close(goid 1) **Bad
content, Aborting Ingest**
04/21/2014 17:03:55.810: node(29377)ERRO:TrickAll.cpp:1506-> ERROR: TrickAll::Close(goid 1) **Aborting
Ingest**
04/21/2014 17:03:55.810: node(29377)ERRO:TrickAll.cpp:1568-> TrickAll::Close(goid 1): ERROR: IngestOK
failed
```

Examine the live/cDVRSessionController log for error messages like the following:

```
04/21/2014 17:03:55.929: (29369)(INFO)profilesStatusConsolidator.js:146 -> FailedProfiles: 1,
totalProfiles: 1. Failure %: 100
04/21/2014 17:03:55.931: (29369)(INFO)profilesStatusConsolidator.js:296 -> Will continue with Posting
status
04/21/2014 17:03:55.932: (29369)(INFO)profilesStatusConsolidator.js:321 -> updateProfilesCountFromApp:
1 .totalProfiles: 1 .crashedProfilesCount: 0
04/21/2014 17:03:55.933: (29369)(INFO)profilesStatusConsolidator.js:328 -> Post the status available
04/21/2014 17:03:55.936: (29369)(INFO)profilesStatusConsolidator.js:480 -> Will post status to
ZK:{"data":{"recordingStatus":{"profile":[{"profileName":"3profile","status":"failed"}],"contentId":"wr
ap","status":"failed"}},"status":"failed"}
```

No PMT In the Feed

Possible Reasons for Failure

There is a bad configuration on the transcoder/encoder for the affected profile.

The source feed to the transcoder failed.

Impact on the End User

There is no PMT in the feed.

The Live/cDVRCaptureApp and the live/cDVRSessionController started to run, but the MPD and .ts files were not created.

The Live/cDVRCaptureApp and the live/cDVRSessionController did not stop until the feed stopped.

Error/Event Messages

Examine the Live/cDVRCaptureApp log for error messages like the following:

```
04/21/2014 17:09:41.957: node(29985)ERRO:TrickAll.cpp:2826-> ERROR: Defaulting Video PID and type.
04/21/2014 17:09:41.957: node(29985)ERRO:TrickAll.cpp:2837-> ERROR:
TrickAll::ProcessInitialMpegData(goid 1): Bitrate cannot be determined.
```

```
04/21/2014 17:19:49.863: node(29985)ERRO:ICaptureSession.h:45-> IOM: [Read timeout occurred. Closing
session]
04/21/2014 17:19:49.864: node(29985)ERRO:Live/cDVRCaptureSession.cpp:428-> No more data on ingest
interface. Failing CaptureSession
04/21/2014 17:19:49.864: node(29985)ERRO:CIF.cpp:1793-> ERROR: Cif::FlushRecords: Not ready: Index
Header not yet written
04/21/2014 17:19:49.864: node(29985)ERRO:CIF.cpp:1477-> ERROR: Cif::WriteClose: Index file incomplete
at end
04/21/2014 17:19:49.864: node(29985)ERRO:CIF.cpp:6145-> ERROR: Cif::WritebackIndex: No Index Header
data
04/21/2014 17:19:49.864: node(29985)ERRO:indexer.cpp:410->
04/21/2014 17:19:49.864: node(29985)ERRO:indexer.cpp:411-> CIndexer: Problems during ingest!!!!
04/21/2014 17:19:49.864: node(29985)ERRO:indexer.cpp:418-> CIndexer: No PMT Found
04/21/2014 17:19:49.865: node(29985)ERRO:indexer.cpp:422-> CIndexer: No Rate was determined
04/21/2014 17:19:49.865: node(29985)ERRO:indexer.cpp:450-> CIndexer: 1 Picture Gaps for 0 bytes or 0.00
seconds (0.00%)
```

Examine the live/cDVRSessionController log for error messages like the following (generated after the feed stopped):

```
04/21/2014 20:21:57.855: (12524)(INFO)live/cDVRCaptureAppSession.js:61 -> IPC data from CaptureApp:{
   "contentId": "wrap",
   "profileName": "3profile",
   "status": "failed"
}
EOM
04/21/2014 20:21:57.857: (12524)(INFO)profilesStatusConsolidator.js:56 -> Got
processStatusUpdate:3profile
04/21/2014 20:21:57.858: (12524)(INFO)profilesStatusConsolidator.js:62 -> updateProfilesCountFromApp
incremented for profile:3profile
04/21/2014 20:21:57.859: (12524)(INFO)profilesStatusConsolidator.js:74 -> shouldWePostStatusNow
returned true
04/21/2014 20:21:57.860: (12524)(INFO)profilesStatusConsolidator.js:204 -> Preparing to Consolidate
Status
04/21/2014 20:21:57.861: (12524)(INFO)profilesStatusConsolidator.js:223 -> Preparing ProfileName:
3profile
04/21/2014 20:21:57.862: (12524)(INFO)profilesStatusConsolidator.js:239 -> Profile: 3profile, status
from map: [object Object]
04/21/2014 20:21:57.863: (12524)(INFO)profilesStatusConsolidator.js:146 -> FailedProfiles: 1,
totalProfiles: 1. Failure %: 100
```

PTS Discontinuity

Possible Reasons for Failure

There is an outage in the Ingest network.

The transcoder/encoder was restarted or reset.

Impact on the End User

The MPD is no longer updating.

The playback has stopped.

No further .ts or .ttml files are generated.

Error/Event Messages

Examine the Live/cDVRCaptureApp log for error messages like the following:

```
04/17/2014 14:14:06.636: node(3495)ERRO:C2ToDashIndexGenerator.cpp:562->
ProcessVideoFragIndexData():562: Unsupported Fragment Duration (8846 seconds) for PTS (2810627849) for
Rep (1510000_video_frag_)
```

```
04/17/2014 14:14:06.636: node(3495)ERRO:C2ToDashIndexGenerator.cpp:621->
ProcessVideoSegIndexData():621: Unsupported Segment Duration (8854 seconds) for PTS (2809907129) for
Rep (1510000_video_seg_1)
04/17/2014 14:14:06.636: node(3495)ERRO:C2ToDashIndexGenerator.cpp:562->
ProcessVideoFragIndexData():562: Unsupported Fragment Duration (8846 seconds) for PTS (2810627849) for
Rep (1510000_video_seg_2)
04/17/2014 14:14:08.637: node(3495)ERRO:CIFConverter.cpp:437-> CIFConverter::GenerateRedisRecord:437 -
Can not find the SIDX{reference_ID: 49, pts: 7901793929} in the pts map to generate the redis record
for the repID[1510000_video_frag_].
04/17/2014 14:14:08.637: node(3495)ERRO:CIFConverter.cpp:149-> CIFConverter::ProcessSIDXRecords:149 -
No records found to build redis record for {repID[1510000_video_frag_], ref_ID[49], pts[7901793929]},
then DROP it!
```

No Audio PID In a Feed

Possible Reasons for Failure

There is a bad channel configuration on the transcoder.

The channel source to the transcoder is losing its audio PID.

Impact on the End User

There is no Audio PID in a feed for one of the profiles in a channel.

There is no timeline for the audio fragments in the MPD, but the video segments and fragments are updating.

HLS playback works normally, with the exception of the profile that lost its audio PID.

HSS playback does not work for any of the profiles.

Error/Event Messages

Examine the Live/cDVRCaptureApp log for error messages like the following:

```
04/18/2014 20:13:38.478: node(21141)ERRO:C2ToDashIndexGenerator.cpp:248-> WARNING: No EBP Implicit seen
in last 20 Secs
```

Examine the live/cDVRSessionController log for error messages like the following:

```
04/18/2014 20:25:19.214: (21133)(INFO)CIFMpdGenerator.js:1095 -> abc-5p: No segments retrieved for
period 1 and adaptation audio_frag_53_1
04/18/2014 20:25:19.216: (21133)(INFO)CIFMpdGenerator.js:1095 -> abc-5p: No segments retrieved for
period 1 and adaptation audio_frag_52_1
```

Examine the LookupService error log for error messages like the following (generated when starting HLS to play the profile without audio PIDs):

```
04/18/2014 20:19:07.600: (21105)(INFO)PlayOutLookupManager.js:463 -> RepID to lookup is:
710000_video_seg_1_1139639856
04/18/2014 20:19:07.603: (21105)(ERRO)LookupTable.js:21 -> Lookup failed with error: null for Channel:
abc-5p
And Redis DB doesn't have the map for the video segment:
127.0.0.1:6379> hget abc-5p 710000_video_seg_1_1139639856
(nil)
```

Same Bitrate on Two Different Profiles

Possible Reasons for Failure

There is a bad channel configuration on the transcoder.

Impact on the End User

Playback works normally for both HLS and HSS within the first TSTV window.

After reaching the TSTV window limit, the playback no longer works for HLS, HSS or DASH-MP4.

Only four of the five expected profiles are present in the MPD file.

Live capture is continuing.

Error/Event Messages

No error messages are sent to the Live/cDVRCaptureApp and live/cDVRSessionController logs.

Examine the LookupService error log for error messages like the following:

```
04/18/2014 18:03:50.210: (14101)(ERRO)LookupTable.js:21 -> Lookup failed with error: null for Channel:
abc-5p
04/18/2014 18:05:07.214: (14101)(INFO)PlayOutLookupManager.js:463 -> RepID to lookup is:
1500000_video_seg_1_416217156
04/18/2014 18:05:07.217: (14101)(ERRO)LookupTable.js:21 -> Lookup failed with error: null for Channel:
abc-5p
04/18/2014 18:05:45.707: (14101)(INFO)PlayOutLookupManager.js:463 -> RepID to lookup is:
1500000_video_seg_1_419820756
04/18/2014 18:05:45.711: (14101)(ERRO)LookupTable.js:21 -> Lookup failed with error: null for Channel:
abc-5p
04/18/2014 18:12:46.045: (14099)(INFO)PlayOutLookupManager.js:463 -> RepID to lookup is:
7500000_video_seg_1_407208156
04/18/2014 18:12:46.047: (14099)(ERRO)LookupTable.js:21 -> Lookup failed with error: null for Channel:
abc-5p
04/18/2014 18:12:46.064: (14102)(INFO)PlayOutLookupManager.js:463 -> RepID to lookup is:
7500000_video_seg_1_409009956
04/18/2014 18:12:46.066: (14102)(ERRO)LookupTable.js:21 -> Lookup failed with error: null for Channel:
abc-5p
```

Different Profiles Have Different Audio Codecs

Possible Reasons for Failure

There is a bad channel configuration on the transcoder.

Impact on the End User

Different profiles in a channel have different audio codecs.

HLS playback works normally.

HSS and DASH-MP4 playback does not work, as there is no timeline in the audio fragments in the MPD file.

Live capture is continuing.

Error/Event Messages

No error messages are sent to the Live/cDVRCaptureApp and Live/cDVRSessionController logs.

When starting an HSS or DASH-MP4 playback, the MPE continuously queries the MPD and the playback freezes.

Profiles In a Channel Are From Different Source Channels

Possible Reasons for Failure

There is a bad channel configuration on the transcoder.

Impact on the End User

The profiles in a channel are from different source channels.

The Live/cDVRCaptureApp and Live/cDVRSessionController processes are running.

The MPD is generated, but there is no timeline for any video or audio segments or fragments.

Playback fails for both HLS, HSS and DASH-MP4.

Error/Event Messages

Examine the Live/cDVRCaptureApp log for error messages like the following:

```
04/18/2014 19:20:50.075: node(18078)ERRO:indexGen.cpp:1456-> IndexGen::NextIndex: TS packet loss for CC
Errors so far 4
```

Examine the Live/cDVRSessionController log for error messages like the following:

```
04/18/2014 19:21:33.522: (18071)(INFO)CIFMpdGenerator.js:1095 -> abc-5p: No segments retrieved for
period 1 and adaptation video_frag_
```

Feed is a VBR Feed

Possible Reasons for Failure

There is a bad channel configuration on the transcoder.

Impact on the End User

The Live/cDVRCaptureApp failed to start the Live channel because it is a VBR feed.

The session controller sent a **Failed** status to the ZooKeeper, but it is still running.

Error/Event Messages

Examine the Live/cDVRCaptureApp log for error messages like the following:

```
04/18/2014 17:09:32.947: node(12029)ERRO:TrickAll.cpp:2331-> TrickAll::ProcessInitialMpegData(goid 1):
ERROR: Appears to be VBR
04/18/2014 17:09:32.947: node(12029)ERRO:indexer.cpp:234-> *** ERROR: NextBlock failed due to bad input
data ***
04/18/2014 17:09:32.947: node(12029)ERRO:LiveCaptureSession.cpp:298-> Stopping LiveCaptureSession
because of bad input data
04/18/2014 17:09:32.947: node(12029)ERRO:TrickAll.cpp:1361-> ERROR: TrickAll::Close(goid 1) **Bad
content, Aborting Ingest**
04/18/2014 17:09:32.947: node(12029)ERRO:TrickAll.cpp:1506-> ERROR: TrickAll::Close(goid 1) **Aborting
Ingest**
04/18/2014 17:09:32.947: node(12029)ERRO:TrickAll.cpp:1568-> TrickAll::Close(goid 1): ERROR: IngestOK
failed
```

Examine the Live/cDVRSessionController log for error messages like the following:

```
04/18/2014 17:09:33.068: (12020)(INFO)profilesStatusConsolidator.js:146 -> FailedProfiles: 1,
totalProfiles: 2. Failure %: 50
04/18/2014 17:09:33.074: (12020)(ERRO)Live/cDVRCaptureAppSession.js:66 -> IPC Channel Error: Error:
write EPIPE, for profile: 1profile
04/18/2014 17:09:33.075: (12020)(ERRO)Live/cDVRCaptureAppSession.js:66 -> IPC Channel Error: Error:
write EPIPE, for profile: 1profile
04/18/2014 17:09:33.078: (12020)(INFO)Live/cDVRCaptureAppSession.js:61 -> IPC data from CaptureApp:{
   "contentId": "abc-10p1",
   "profileName": "2profile",
   "status": "stopped"
}
04/18/2014 17:09:50.871: (12020)(INFO)profilesStatusConsolidator.js:480 -> Will post status to
ZK:{"data":{"recordingStatus":{"profile":[{"profileName":"1profile","status":"failed"},{"profileName":"
2profile","status":"stopped"}],"contentId":"abc-10p1","status":"failed"}},"status":"failed"}
```

PTS Discontinuity in the Feed

Possible Reasons for Failure

There is a presentation timestamp (PTS) discontinuity in the feed. This can occur in rare instances in the Digital Content Manager (DCM).

Impact on the End User

The playback session (HLS by QuickTime/HSS by Silverlight/DASH-MPE by bitdash player) stops, but it resumes playing after a restart.

Resolution

There is no resolution for this problem at this time.

VOD Injest-Recording Status Fails with one Failed Profile

Possible Reasons for Failure

When more than one profile is configured

Impact on the User

If one profile fails during the injest for any reason, for example (source file not found or source file format not recognized, the entire asset is considered failed. This triggers a relocation of the injest task to another worker until the maximum relocation is exhausted. If all the relocation attempts fail to injest, then the asset is marked as failed.

Resolution

There is no resolution for this problem at this time.

Multicast Encoder does not work between Encoder and MCE

Scenario

IGMPv2 (no source IP), where the MCE and encoder IP addresses are on different subnets but on a single flat VLAN. e.g. MCE: 192.168.2.11, encoder: 10.10.1.1. No routed network here, a single layer 2 domain. Multicast should work between encoder and the MCE.

Possible Reasons for Failure

linux kernel by default filters out packets from different subnets - to protect against sources that it doesn't believe traffic could be coming from (for example, different subnets if there's no route to that subnet). tcpdump shows multicast packets being received because it's a flat VLAN, but they get dumped before reaching the live capture application; MCE reports a data timeout on the channel.

Impact on the User

Multicast encoder does not work between encoder and MCE.

Resolution

Disable the filter for the ethernet interface where multicast is incoming. (add the line net.ipv4.conf.eth1.rp_filter=0 to /etc/sysctl.conf and restart the network.

MCE Fail to Capture When the Feed is Changed to 25fps

Scenario

When the DCM feed configuration is changed from 29.7 fps to 25fps, MCE fail to detect EBP's in feed and capturing fails.

Possible Reasons for Failure

Changing the frame rate in the DCM while the channel is running. Changing the dynamic configuration on the DCM is not supported.

Workaround

If the frame rate is changed in the DCM while the channel is running, restart the channel.

Error/Event Messages

Examine the log for error messages like the following:

```
[admin@MCE-08 errorlog]$ grep CHAN1051 LiveCaptureApp-errorlog.current
2015-10-12T22:00:23.134Z: 19279 CIFGenerator CIFDbStore.cpp:729 [Console] ERROR ->
[liveCaptureApp|livetmp/CHAN1051:HD03] CifDbStore (0x1a98c80), No SIDX arrived for representation
(1700000_audio_frag_101) in last 60 seconds
2015-10-12T22:00:23.135Z: 19279 CIFGenerator CIFDbStore.cpp:729 [Console] ERROR ->
[liveCaptureApp|livetmp/CHAN1051:HD03] CifDbStore (0x1a98c80), No SIDX arrived for representation
(1700000_cc_frag_eng_) in last 60 seconds
2015-10-12T22:00:23.135Z: 19279 CIFGenerator CIFDbStore.cpp:729 [Console] ERROR ->
[liveCaptureApp|livetmp/CHAN1051:HD03] CifDbStore (0x1a98c80), No SIDX arrived for representation
(1700000_i-frame) in last 60 seconds
```

MCE Troubleshooting Tools

The following tools are used for troubleshooting the MCE.

udpCapture

Purpose:

Capture the multicast live feed and writing to udpDataFile, and verify if client can receive multicast packets from source.

Usage:

```
./udpCapture [-t] <ip address> <port number> <eth interface> [<source ip>]
Mandatory arguments:
<ip address>: multicast address
<port number>: multicast port
<eth interface>: the client interface which will receive the feed
Optional arguments:
[source ip]: multicast source ip address
[-t]: a 4-byte header with the packet arrival time in milliseconds since the start of capture will be
prepended to each 188-byte record.
Example-1?
~ admin]#./udpCapture 232.10.1.1 1002 eth1 99.1.1.2
receiving on 232.10.1.1:1002 99.1.1.2 ifindex 3 (eth1) and writing to udpDataFile
received 3934840 bytes in 11 seconds (2861 Kbps)
received 8197364 bytes in 22 seconds (2980 Kbps)
received 12459888 bytes in 33 seconds (3020 Kbps)
received 16722412 bytes in 44 seconds (3040 Kbps)
... ... ...
Example-2:
~ admin]# ./udpCapture -t 232.10.1.1 1002 eth1 99.1.1.2
receiving on 232.10.1.1:1002 99.1.1.2 ifindex 3 (eth1) and writing to udpDataFile
received 4213832 bytes in 11 seconds (3064 Kbps)
received 8477672 bytes in 22 seconds (3082 Kbps)
received 12738880 bytes in 33 seconds (3088 Kbps)
received 17002720 bytes in 44 seconds (3091 Kbps)
... ... ...
```

vInfo

Purpose:

Get information about MPEG-2 transport stream, such as basic PID, codec, bitrate,GOP structure,etc.

Usage:

```
./vInfo [-v] [-a] [-p] tsfile1 tsfile2 tsfile3 ...
Optional arguments:
[-a]: the entire sample will be scanned, not just part of it
[-v]: additional (verbose) information will be given,like the packet number found PAT or PMT
[-p]: check is made for the presence of PowerKey content
Example-1:
~ admin]#./vInfo p10001.ts
Details for p10001.ts:
PAT:
1 Program
PMT:
PMT PID is 33
PCR PID is 32
Program PID Loop, 2 PIDs:
PID 32 (0x020): Type: 27 (0x1B): AVC/h.264 VIDEO
PID 40 (0x028): Type: 15 (0x0F): AAC AUDIO eng
Rate:
4,511,000 bps
Length:
338,339,652 bytes
600.03 seconds or 10:00
Video:
H.264 MAIN L4.0 4:2:0 Progressive 1280x720 Square
GOP Structure:
First 10:
PBBPBBPBB
IBBPBBPBBPBBPBB
IBBPBBPBBPBBPBB
IBBPBBPBBPBBPBB
I*PBBPBBPBBPBB
IBBPBBPBBPBBPBB
IBBPBBPBBPBBPBBPBBPBBPBBPBB
IBBPB
I*PBBPBBPBBPBB
IBBPBBPBBPBBPBB
Calculated Frame Rate is 29.97fps
In first 5:00/10 lines:
GOPs: 615 (IDRs: 150)
GOP length: 1 - 32 (Average 15)
All Frames
About 75.9 PCRs/sec
1 Audio:
82: AUDIO id 0: sample rate 48000 bitrate 128250 channels 2 codec info 0x4c80
PID 40 AAC AUDIO sample rate 48kHz bit rate 128250bps channels 2 codec info 0x4c80
Scrambling:
No scrambling in first 5:00 of stream
Example-2:
~ admin]# ./vInfo -v p10001.ts
Details for p10001.ts:
PAT:
Found PAT at packet 296
Version 7
TSID is 1
```

```
1 Program
0: Program Number is 10
0: PMT PID is 33 (0x021)
PMT:
Found PMT at packet 515
PMT PID is 33
Version 7
PCR PID is 32
Program PID Loop, 2 PIDs:
PID 32 (0x020): Type: 27 (0x1B): AVC/h.264 VIDEO
PID 40 (0x028): Type: 15 (0x0F): AAC AUDIO eng
Rate:
4,511,000 bps (at packet 1198 or 219K)
Length:
338,339,652 bytes
600.03 seconds or 10:00
Video:
H.264 MAIN L4.0 4:2:0 Progressive 1280x720 Square
GOP Structure:
First 10:
PBBPBBPBB
IBBPBBPBBPBBPBB
IBBPBBPBBPBBPBB
IBBPBBPBBPBBPBB
I*PBBPBBPBBPBB
IBBPBBPBBPBBPBB
IBBPBBPBBPBBPBBPBBPBBPBBPBB
IBBPB
I*PBBPBBPBBPBB
IBBPBBPBBPBBPBB
Calculated Frame Rate is 29.97fps
In first 5:00/10 lines:
GOPs: 615 (IDRs: 150)
GOP length: 1 - 32 (Average 15)
All Frames
About 75.9 PCRs/sec
1 Audio:
82: AUDIO id 0: sample rate 48000 bitrate 128250 channels 2 codec info 0x4c80
PID 40 AAC AUDIO sample rate 48kHz bit rate 128250bps channels 2 codec info 0x4c80
PID 40: About 46.9 PUSIs/sec
Scrambling:
No scrambling in first 5:00 of stream
```

3). checkEbps

```
Introduction: Check if transport stream has video/audio EBPs, as well as the the number of them
Usage:
./checkebps profile1.ts profile2.ts profile3.ts ... ...
Example-1:
~ admin]# ./checkEbps p10001.ts
Looking for EBPs in the input file p10001.ts
Profile 1 stats
Number of Video EBPs: 299
Number of Audio EBPs: 373
First Video PTS 6337472130
Fragment Delta: 2 seconds
Segment Delta: 10 seconds
Done.
Example-2:
~ admin]# ./checkEbps p10001.ts p10004.ts
Looking for EBPs in the input file p10001.ts
Profile 1 stats
Number of Video EBPs: 299
Number of Audio EBPs: 373
First Video PTS 6337472130
Fragment Delta: 2 seconds
Segment Delta: 10 seconds
```

```
Looking for EBPs in the input file p10004.ts
Profile 2 stats
Number of Video EBPs: 299
Number of Audio EBPs: 373
First Video PTS 6337472130
Fragment Delta: 2 seconds
Segment Delta: 10 seconds
Done.
```

scte35dump

Purpose:

Dumps out any SCTE-35 information in the specified file, which can be an SPTS or MPTS.

Usage:

```
./scte35dump input_file
Example-1:
~ admin]# ./scte35dump DR_output_2864000.ts
1 Program(s):
ProgNo 02 has SCTE 35 on PID 43
Rate::Compute(goid 0): WARNING: Bit Rate=3208248 Delta Rate=3001253 Diff=6%
Rate::Compute(goid 0): WARNING: PCR(12)=139231 and PCR(41)=531611
Rate::Compute(goid 0): WARNING: PCR sequence changed. Restarting rate calc.
Rate::Compute(goid 0): WARNING: Bit Rate=2972635 Delta Rate=3163053 Diff=6%
Rate::Compute(goid 0): WARNING: PCR(1227)=16733090 and PCR(1297)=17631766
Ignoring.
Rate::Compute(goid 0): WARNING: Bit Rate=2999367 Delta Rate=1656714 Diff=44%
Rate::Compute(goid 0): WARNING: PCR(2037)=27555172 and PCR(2100)=29099375
Rate::Compute(goid 0): WARNING: PCR sequence changed. Using current rate.
WARNING: Sample appears to be VBR. Setting rate to zero.
ProgNo 00 has initial PCR of 37,972 (or 126 PTS-equivalent)
ProgNo 00 has initial PTS of 70,503 (or 0.78 seconds after first PCR)
Searching...
2: SCTE35(2): Not splice_insert!
21,572: SCTE35(2): Not splice_insert!
23,540: SCTE35(2): Not splice_insert!
1,268,665: SCTE35(2): Not splice_insert!
1,328,706: SCTE35(2): Not splice_insert!
1,941,332: SCTE35(2): Not splice_insert!
1,971,375: SCTE35(2): Not splice_insert!
2,908,754: SCTE35(2): Not splice_insert!
2,968,926: SCTE35(2): Not splice_insert!
3,620,494: SCTE35(2): Not splice_insert!
3,680,748: SCTE35(2): Not splice_insert!
4,554,930: SCTE35(2): Not splice_insert!
4,585,017: SCTE35(2): Not splice_insert!
100%
Summary:
ProgNo 02 had 13 splice_inserts for 0 avails: 0 OP, 0 IP, 0 Valid IP
```

IndexCheck

Purpose:

Check the index details for CDN Index data file.

Usage:

```
./IndexCheck [-v|-V|-x|-h|-t] IndexFileName
Optional arguments:
-v: Verbose output
-V: Verbose with NPTs
-x: Quit on first error found
-h: Show header
-t: Show trailer
Example-1:
~ admin]# ./IndexCheck -h content_obj_idx
WARNING: Cannot figure out the 1x filename
GetMetaDataFormat: Identified as CDN Index data
Index writeback HAS been completed
Video Index File
Version: 2.0.1
Creator: Cisco Systems
File Header Checksum : OK
File Header size : 64 bytes, incl. 1 byte post-pad
Index Header size : 8132 bytes, incl. 6764 bytes post-pad
Total Header size : 8196 bytes
=== Index Header ===
AssetInformation:
CreationVendorID : 0x00000C
AssetIngestTime : 2016-05-19 09:58:01.770 UTC
IndexCreationTime : 2016-05-19 09:58:01.770 UTC
ProgramVersion : Software Version 0.0a
SourceFileName : 0x0002f56aaea03618
FileWrapperType : MPEG-2 Transport Stream
TransportPacketSize : 188 bytes
SyncByteOffset : 0
TransportBitRate : 3,599,957 bps
TransportStreamType : H.264 video stream plus zero or more audio streams
MaximumIFrameDistance : 32 frames
VideoHorizontalSize : 1280 pixels
VideoVerticalSize : 720 pixels
VideoFrameRateTicks : 3003 90 KHz clocks
VideoFrameRateTimeScale : 90,000 Hz
TrickPtsDtsDelta : 0 90 KHz clocks
PtsDtsCalculationMethod : Calculated from the end of the frame
InitialDecodingDelay : 0 90 KHz clocks
TrickDelayFromEOF : 30,030 90 KHz clocks
TransportStreamCount : 1
ElementaryStreamCount : 3
SubFileCount : 1
PcrIntervalPacketCount : 89 x 188 byte cells
SCTE35RecordCount : 0
*** SubFileDynamic : YES ***

*** OpenForWrite : NO ***
TransportStreamInformation:
TransportStreamProgramNumber : 3
TransportStreamPmtPID : 048 (0x030)
TransportStreamPcrPID : 049 (0x031)
TransportStreamVideoPID : 049 (0x031)
TransportStreamAudioPID : 052 (0x034)
TransportStreamAudioPID : 053 (0x035)
TransportStreamSCTE35PID : 000 (0x000)
```

```
ElementaryStreamInformation:
ElementaryStreamType : 27
ElementaryStreamPID : 049 (0x031)
ElementaryStreamDescriptor : 06 01 02 28 04 4D 40 1E 3F 0E 03 C0 1C F0 97 00 E9 07 10 83 0A 41 85 02 41
ElementaryStreamSeqParamSet :
ElementaryStreamPicParamSet :
ElementaryStreamID : 0xE0
... ...
... ...
```

Example-2:

```
~ admin]# ./IndexCheck -x content_obj_idx
WARNING: Cannot figure out the 1x filename
GetMetaDataFormat: Identified as CDN Index data
Index writeback HAS been completed
Video Index File
Version: 2.0.1
Creator: Cisco Systems
File Header Checksum : OK
File Header size : 64 bytes, incl. 1 byte post-pad
Index Header size : 8132 bytes, incl. 6764 bytes post-pad
Total Header size : 8196 bytes
*** SubFileDynamic : YES ***
*** OpenForWrite : NO ***

ERROR: Index Header: Unidentified tag
```

vDump4

Purpose:

Used to dump the given stream detailed information such as I/B/P frames, GOP, PTS, DTS, EBP timestamps, etc.

Usage:

```
./vDump4 [-n] [-v] [-i] [-p] [-g] [-s] [-r] input_file [video_pid]
Optional arguments:
[video_pid]: video_pid will be computed if not specified
-v is verbose output: shows NULL pkts with -a
-i uses SCTE35 splice insert commands
-p adds PCR output
-g is GOP short output (use alone or with -s)
-1 is 1-line, PIC only output
-s adds a summary at the end.
-n turns off everything (first, use with -s).
-x don't try and compute rate.
-a adds non-video PID data.
-d show PTS vs PCR deltas.
-r uses reverse trick packet numbering.
-e show EBP timestamps.
```

Example-1:

```
~ admin]# ./vDump4 -s p10008.ts
ERROR(0): PUSI not set on first video
AUDIO(1): PID: 40 PTS: 6302798498
AUDIO(10): PID: 40 PTS: 6302800418
AUDIO(22): PID: 40 PTS: 6302802338
AUDIO(31): PID: 40 PTS: 6302804258
AUDIO(43): PID: 40 PTS: 6302806178
AUDIO(54): PID: 40 PTS: 6302808098
AUDIO(63): PID: 40 PTS: 6302810018
PES(64): len=0 0x84 0xd0 PTS: 6302888081 DTS: 6302879072
AU-DELIM(64): ----- I,P -----
SEI(64)
```

```
SEI(64)
SLICE(64): INVALID PPS ID/NOT SEEN 0
AUDIO(75): PID: 40 PTS: 6302811938
PES(79): len=0 0x84 0x90 PTS: 6302882075 (-6006)
AU-DELIM(79): ----- I,P,B -----
SEI(79)
SEI(79)
SLICE(79): INVALID PPS ID/NOT SEEN 0
PES(82): len=0 0x84 0x90 PTS: 6302885078 (+3003)
AU-DELIM(82): ----- I,P,B -----
SEI(82)
SEI(82)
... ...
... ...
Summary:
Total Frames: 1788
I Frames: 125
P Frames: 505
B Frames: 1158
Min GOP: 1
Max GOP: 27
Average GOP: 14
Packets: 29890
I Packets: 8412680
P Packets: 1358981930
B Packets: 1068935
Bytes: 5619320
I Bytes: 1581583840
P Bytes: 2085532376
B Bytes: 200959780
Avg GOP: 44954 bytes
Avg Frame: 3142 bytes
Avg I-Frame: 12652670 bytes
Avg P-Frame: 4129767 bytes
Avg B-Frame: 173540 bytes

Based on all muxed packets:
Max I-Frame: 27448 bytes at #5566 (0.293s)
Max P-Frame: 11656 bytes at #22583 (0.124s)
Max B-Frame: 3948 bytes at #10871 (0.042s)
Min PTS: 6302882075 at packet 79 with pattern BT
PCR at zero: 1890837823016 or 6302792743 at 90kHz
Lead: 89332 or 0.99 secs
Max PTS: 6308284472 at packet 29841 with pattern BT
PCR at end: 1892458344004 or 6308194480 at 90kHz
Lag: 92995 or 1.03 secs
PCR at end calculations:
From start: 1892458343548 (+1620520532 or 60.02s)
From nearby: 1892458344004 (+1620520988 or 60.02s)
Seconds: 60
Frames/Sec: 29.8
I-Frames/Sec: 2.0
```

Troubleshooting the MPE

- General Playout Problems, page 165
- Problems with Captions/TTML, page 165
- Problems with ESAM, page 166
- Problems with DRM, page 166

- Troubleshooting the SAL, page 169

General Playout Problems

If you experience a general problem with playout, take the following steps to diagnose and correct the problem:

1. Using **wget**, verify that the manifests can be retrieved from the MPE-Worker.
2. Examine the transaction log for 404/500 errors for the manifest and segment/fragment requests when attempting the playout.
3. Examine the ingest log for 404/500 errors for the MPD and TS segment requests.
4. Examine the MPD (using **wget** on the URL in the ingest log) and verify that the correct adaptation sets are present:

- **video_seg_2** and **video_seg_1** for HLS playout
- **i-frame** for HSS and HLS sudo ifupmode
- **audio_frag_*** and **video_frag_*** for HSS playout
- **audio_frag_*** and **video_frag_auto*** for Dash-mp4 playout

5. In the adaptation sets, verify that the segment timeline is present:

```
<SegmentTimeline>
    <S t="2205403578" d="900900" r="17"/>
</SegmentTimeline>
```

6. In the adaptation sets, verify that the **t** values within the timelines are all close to each other. For example, if the video_frag_* segment timeline has **t** set to **5000000**, but the audio_frag_* timeline has **t** set to **7000000**, those values are too far out of sync. Change one or both of the *t* values to be more in sync.
7. Examine the MPD and look at the bandwidth of the source feed (the "bandwidth=" value in the appropriate representation for an adaptation set). Verify that the bitrates configured for variant playlists are within 5% of the bandwidth of the source feed.
8. To ensure that the variant configuration is being correctly propagated from the VMP-M GUI to the MPE-Worker, examine the odesdk_log in the /errorlog directory with DETAIL logs set. Verify that the correct configurations for the given manifest URL are present:

```
Apr 15 14:34:10 sjc-xdm-108 encapsulator[10702]: File: src/transforms/TransformMap.cpp Funct: putRoot
Line: 31 TRACE: putRoot /ode/hss/asset3.ismc
Apr 15 14:34:10 sjc-xdm-108 encapsulator[10702]: File: src/AssetTransform.cpp Funct: logMetadata Line:
326 TRACE Metadata:variantUrl=/ode/hss1/asset3.ismc variantId=ipad1 assetId=2000 manifestVersion=2
CifId=asset.mpd parentManifestId=2000 keyId=
Apr 15 14:34:10 sjc-xdm-108 encapsulator[10702]: File: src/AssetTransform.cpp Funct: logMetadata Line:
351 TRACE vidVector:3348998, size=1 audVector:60000, size=1
```

9. Verify that **max-age=0** is set for Manifests in the asset resolver options (not **max-age=3600**; not necessary for Chunks).

Problems with Captions/TTML

If captions are not being displayed, take the following steps to diagnose and correct the problem:

1. Verify that the original feed has captions.
2. Verify that the **CC** button is **ON** in the player.

If the captions are not aligned with the audio, check the original feed for the same problem.

If you see escape sequences such as **>** instead of **>** and other symbols, that is a known player issue, and it must be addressed by the player vendor or developer.

Problems with ESAM

If an advertisement is not honored, take the following steps to diagnose and correct the problem:

1. Verify that the POIS server is up.
2. Check the connection between the POIS server and the DCM.
3. Check the connection between the POIS server and the MCE.
4. If you can access the MPD file, determine whether <EventStream> is created with value=”esam_pois”.

- Use **wget** to capture the HLS manifest and look for the “#EXT-X-DISCONTINUITY” and “#EXT-X-SPLICE-EXIT” tags.
- Use **wget** to capture the HSS manifest and look for <StreamIndex> with Name=”scte35”.

Problems with DRM

If playout failed, take the following steps to diagnose and correct the problem:

1. Check the web-engine error logs for any indication of errors.
2. Check web-engine transaction logs to determine whether the client retrieved only the manifest, or if it also retrieved the segments.
3. Check the transaction logs to determine whether the key retrieval was successful.
4. If only the manifest is retrieved, then the problem could be a general playout issue such as error in the manifest file creation, or it could be a content encryption error. Examine the error logs for more information.
5. If a segment is also retrieved, then the problem could be incorrectly encrypted content, or the client might be unable to retrieve the key given the key URI in the manifest. If this is the problem, the player might generate a message like, “Unable to decrypt content.”
6. In each of these cases, you can further diagnose the problem by manually retrieving the manifest files and the corresponding segments, using **wget** or **curl**, and then analyzing the output.
7. When analyzing a PlayReady manifest file:

- Look for the <ProtectionHeader> sample encryption header in the manifest.
- Look for the <ContentProtection> sample encryption header in the DASH-MP4 mpd.

For example:

```
<ContentProtection
    schemeIdUri="urn:uuid:edef8ba9-79d6-4ace-a3c8-27dcd51d21ed">
    <cenc:pssh

xmlns:cenc="urn:mpeg:cenc:2013">AAAAU3Bzc2gAAAAA7e+LqXnWSs6jyCfc1R0h7QAAADMIARIQdXi1QWdbRuS+qFdVM/fqoho
LYnV5ZHJta2V5b3MiEG4pW96+VkgJky3kjhG7RAI=</cenc:pssh>
    </ContentProtection>
```

- For HLS, look for the EXT-X-TAG tag.

For example:

```
<Protection>
    <ProtectionHeader
SystemID="{9A04F079-9840-4286-AB92-E65BE0885F95}">hAMAAAEAAQB6AzwAVwBSAE0ASABFAEEARABFAFIAIAB4AG0AbABuA
HMAPQAiAGgAd...
</Protection>
```

8. When analyzing a segment, compare the retrieved segment to the same content which is retrieved with no encryption, if it is available. If the sizes are the same, then encryption is not occurring. If the sizes are different, encryption is VMPt likely occurring.

9. Verify that the configuration is correct. The Asset Resolver file must use the correct regular expression (regex) matching pattern for the given request. Each Asset Resolver entry must include a <ContentProtectionProfileName> entry with a name that matches the DRM type name assigned within the KmsProxy config.

If the web-engine logs indicate a failure to acquire the key through the proxy, take the following steps to diagnose and correct the problem:

1. Verify that the supervisorctl status shows the drm-system_app is in **RUNNING** state.

2. Examine the /var/log/opt/cisco/VMP/errorlog/kmsproxy-errorlog.current error log for recent errors.

3. Verify that the relevant key profile configurations were pushed to the proxy by examining the /opt/cisco/VMP/node/lib/node_modules/drm-system/kmsproxy/test/ directory: source test.curl and kpAll list the configuration details for the key profile.

4. If the following shows as "initComplete":false, then connectivity to the Irdeto KMS is not working:

```
irdeto/IrdetoHss/pr-aes-128/keysCached=0
{"name":"IrdetoHss","properties":{"description":"Irdeto HSS Mike",
"drmType":"pr-aes-128","type":"irdeto",
"keyAcquisition":{"uri":"https://173.36.199.89:8092/livedrmservice/livedrmservice.asmx",
"userName":"cisco@twc.com","passPhrase":"ABuB73s05FSR",
"account":"twc","clientCert":"","caCert":"","clientKey":"","protocol":"https:","basePath":"/livedrmserv
ice/livedrmservice.asmx",
"host":"cld3.man.entriq.net","port":"443"},
"initComplete":true}}
```

5. If there are errors in the kmsproxy log file that indicate a lack of connectivity, or if the cache in the proxy is empty (with **curl** commands as described in test.curl), then check the connectivity to the KMS. You can also verify the connectivity directly using the **curl** commands in test.curl, such as:

```
curl -k --request POST -H 'Content-type: text/xml' -H 'SOAPAction:
\"http://man.entriq.net/livedrmservice/Get\Settings\"' -d @Get\Settings.xml https://
cld3.man.entriq.net:443/livedrmservice/livedrmservice.asmx
```

Troubleshooting DRM Types

Insys

On the PAM check that the Insys profile has the correct urls for key acquisition uri ("uri") and the authorization uri ('authUri') and other credentials – the curl commands in the test.curl file can be used as a guideline for exercising these rest apis.

```
Example :
keyAcquisition":{"uri":"http://<ipaddr>/Soap/Kms.svc","userName":"user","passPhrase":"pass","serviceId"
:19,"authUri":"<ipaddr>/Soap/Authentication.svc"
```

The redis on the PAM is used for persistence of the mapping of the VMP contentId to the Insys KeyId. In some cases, it may be required to clear this redis entry so that there is no chance of persisting expired keys.

1. From command prompt enter 'redis-cli'

2. Display the mapping – example:

```
127.0.0.1:6379> hgetall drm:insysHss:CiscoTest2
1) "keyId"
2) "541ea387-6ec6-4a46-92ac-bc47ed336d68"
```

3. Delete the entry – example:

```
127.0.0.1:6379> del drm:insysHss:CiscoTest2
(integer) 1 1
```

4. supervisorctl restart drm-system

VGC

On the PAM, check that the VGC profile has the correct url for key acquisition from the abre REST API – the curl commands in the test.curl file can be used as a guideline for exercising these rest apis.

```
Example : "keyAcquisition":{"uri":http://<restapi-host>:5701/drmapi/package
```

Check the REST api VM to make sure the service has started and that it is configured to point to the correct Keystore host:port and the ECMS host:port. Refer to the ABR Encryptor Installation and Configuration guide for more details.

1. For Live, the redis on the PAM is used for persistence of the reference mapping of the PTS in the playlist to the corresponding UTC rotation point for each Live stream. In some cases, it may be required to clear this redis entry so that the PTS to UTC mapping can be reset properly.

2. From the command prompt, enter 'redis-cli'

3. Display the mapping – example:

```
127.0.0.1:6379> hgetall drm:vgcHls:CiscoTest1
1) "rotationRefPointUTC"
2) "2015-01-14T05:43:44Z"
3) "rotationRefPointPTS"
4) "127909280160000"
5) "refPointOffset"
6) "127909263060000"3) Delete the entry – example :
127.0.0.1:6379> del drm:vgcHls:CiscoTest1
(integer) 1
```

4. supervisorctl restart drm-system

EZDRM

On the PAM, make sure the EZDRM profile has the correct urls for the Key Service URI ("uri"), Username and Passphrase The curl commands in the test.curl file can be used as a guideline for exercising these rest apis.

```
Example :
keyAcquisition":{"uri":"http://<ipaddr>/Soap/Kms.svc","userName":"user","passPhrase":"pass","serviceId"
:19,"authUri":"<ipaddr>/Soap/Authentication.svc"
```

The redis on the PAM is used for persistence of mapping the VMP contentId to the Insys KeyId. In some cases, it may be required to clear this redis entry so that there is no chance of persisting expired keys.

1. From the command prompt, enter 'redis-cli'.

2. Display the mapping – example:

```
127.0.0.1:6379> hgetall drm:ezdrm:vod1
 1) "keyId"
 2) "tTRAsUaUXRaDQ78WNyZBwg=="
```

3. Delete the entry – example:

```
127.0.0.1:6379> del drm:ezdrm:vod1
(integer) 1 1
```

4. supervisorctl restart drm-system

BuyDRM

On the PAM, make sure the BuyDRM profile has the correct urls for Key Service URI (“uri”), Server key and User Key. The curl commands in the test.curl file can be used as a guideline for exercising these rest apis.

```
Example :
keyAcquisition":{"uri":"http://<ipaddr>/Soap/Kms.svc","userName":"user","passPhrase":"pass","serviceId"
:19,"authUri":"<ipaddr>/Soap/Authentication.svc"
```

The redis on the PAM is used for persistence of mapping the VMP contentId to the Insys KeyId. In some cases, it may be required to clear this redis entry so that there is no chance of persisting expired keys.

1. From the command prompt, enter ‘redis-cli’
2. Display the mapping – example:

```
127.0.0.1:6379> KEYS drm:buydrm:vod1
 1) "drm:buydrm:vod1"
 127.0.0.1:6379> hgetall drm:buydrm:vod1
 1) "kid"
 2) "7578b541-675b-46e4-bea8-575533f7eaa2"
 3) "cid"
 4) "6e295bde-be56-4809-932d-e48e11bb4402"
 5) "mid"
 6) "93711ffc-a557-43ad-b220-17239d488f98"
```

3. Delete the entry – example:

```
127.0.0.1:6379> del drm:buydrm:vod1
(integer) 1 1
```

4. supervisorctl restart drm-system

Troubleshooting the SAL

- Restarting the SAL, page 169
- The SAL Port, page 169
- The SAL Log File, page 169
- The SAL Storage, page 170

Restarting the SAL

To restart the SAL, enter the following command:

```
supervisorctl restart StorageMain
```

The SAL Port

The SAL runs on port 5123 on the localhost.

The SAL Log File

The SAL log file is located in the /var/log/opt/cisco/VMP/errorlog/StorageMain/ directory.

```
ls -l /var/log/opt/cisco/VMP/errorlog/StorageMain/storage-init.log.*
```

The current log file is the sal-init.log.current file.

To see what is going on within the SAL, enter the following command:

```
tail -F /var/log/opt/cisco/VMP/errorlog/StorageMain/storage-init.log.current
```

Log levels are configured on the “log_level” property in the /etc/opt/cisco/VMP/StorageMain/storage_server_config.json file:

```
{
    "server_port" : 5123,
    "monitor_time_interval" : 2,
    "pid_file_path" : "/var/run/storage-server/storage-server.pid",
    "log_level" : "log_info",
    "log_socket_path" : "/tmp/StorageMain"
}
```

The SAL supports the following log levels:

- log_info—When enabled, prints critical + error + warning + info messages. This is the default log level. If the “log_level” property in the storage_server_config.json file is incorrect or unknown, the SAL uses this log level.
- log_critical—When enabled, prints only critical error messages.
- log_error—When enabled, prints critical + major error messages.
- log_warning—When enabled, prints critical + error + warning messages.
- log_trace—When enabled, prints critical + error + warning + info + trace error messages.
- log_detail—When enabled, prints all messages: critical + error + warning + info + trace error + detail messages.

To change the log level, change the “log_level” property to a different level, then restart the StorageMain process using the **supervisorctl** command.

Supervisor logs for the SAL are located in the /var/log/supervisor/StorageMain.log file. All uncaught exceptions are written to the supervisor file. If something basic is not working, check the supervisor log to see if there are any uncaught exceptions.

The SAL Storage

This release of SAL supports NFS versions 3.0 and 4.0.

There is no default NFS version for the SAL. The version field is mandatory and must be set to 3.0 or 4.0. However, if you ask for a 4.0 NFS mount, and your NFS server does not support version 4.0, the SAL uses the lower version supported by your NFS server.

The SAL maintains state information. That is, if the SAL crashes and comes back up, it remembers the previous mounts and returns to its pre-crash state.

The SAL monitors all of the shares it has mounted. If a mount failure occurs, the SAL sends an HTTP notification to a callback URL. The callback URL is sent to the SAL as a query string in the request POST URL. The SAL sends the notification to the service agent using the callback URL. The service agent in turn writes the notification to the ZooKeeper.

When an NFS server goes down, the SAL monitors the failed mount points and tries to automatically remount them when the NFS server comes back online. The monitoring does no time out; the SAL monitors the failed mount points indefinitely.

This release does not support the reporting of NFS usage statistics.

The SAL uses a REST API to delete and unmount all mount points. To unmount all mount points, enter the following command:

curl -i -X DELETE -H Content-Type:application/json /v1/delete_all_storage

This command unmounts all mount points and removes entries for those mount points from the SAL configuration.

If the SAL is not able to mount an NFS server, take the following steps to diagnose and correct the problem:

1. Examine the sal-init.log.current file for recent ERROR and WARNING messages.
2. Examine the mount command that the SAL is using to mount the NFS server.

- Try to mount the NFS server by entering the SAL mount command manually.
- Try to mount the NFS server by entering the following command:

mount -t nfs -o vers=3 nfs_server_ip:/share *mount_path*

3. Examine the StorageMain.log supervisor log for uncaught exceptions in the code.
4. Verify that the share path and NFS version are valid.

The following sample JSON files demonstrates how to create a storage mount using the SAL. Additional sample JSON and test scripts are located in the 2.3/storage/init/test directory.

```
{
    "SALMount": [
        {
            "id": "pos_nfs_1",
            "name": "1",
            "type": "smnasmediasource",
            "owner": "smtenants.smtenant.system",
            "properties": {
                "share": "/data",
                "version": "4.0",
                "servers": [
                    {
                        "rangeStart": "127.0.0.1",
                        "rangeEnd": "127.0.0.1"
                    }
                ],
                "description": "nas storage",
                "numMounts": 2
            }
        },
        {
            "id": "pos_nfs_2",
            "name": "2",
            "type": "smnasstore",
            "owner": "smtenants.smtenant.system",
            "properties": {
                "share": "/Public",
                "version": "3.0",
                "servers": [
                    {
                        "rangeStart": "172.25.137.11",
                        "rangeEnd": "172.25.137.11"
                    }
                ],
                "description": "nas storage",
                "numMounts": 2
            }
        }
                "description": "nas storage",
                "numMounts": 2
```

```
            }
        }
    ]
}
```

Troubleshooting the AWM

Use the following tools and procedures to troubleshoot the Asset Workflow Manager (AWM).

- AWM Troubleshooting Tools, page 172
- AWM Troubleshooting Tips, page 175

AWM Troubleshooting Tools

- Asset Management API and Status, page 172
- AWM Statistics, page 173
- AWM Error Log, page 174
- AWM Transaction Log, page 174

Asset Management API and Status

For each Asset Workflow Template (AWT) in a service instance, the AWM publishes an asset management Use-API to the DocServer. The Use-API document includes the following information:

- AssetWorkflow Use-API status: **Ready** or **Failed**
- URL to create assets

AssetWorkflow API Format

`http://am-cepName-serviceInstanceName.base_domain:port/version/assetworkflows/awtName/assets`

Sample AssetWorkflow API Format

`http://am-cep1-live1.VMP.com:7001/v1/assetworkflows/nationalChGrp/assets`

Sample Asset API Output

```
[
    {
        "assetMgmtUrl": "http://am-cep1-live1.VMP.com:7001/v1/assetworkflows/live1/assets/CiscoTest1",
        "contentId": "CiscoTest1",
        "output": [
            {
                "type": "hls",
                "url": "http://live-ca.VMP.com/nodvr-live/CiscoTest1/CiscoTest1.m3u8"
            },
            {
                "type": "hls",
                "url": "http://live-ca.VMP.com/nodvr-live/CiscoTest1/appleTv.m3u8",
                "version": "4"
            },
            {
                "type": "hls",
                "url": "http://live-ca.VMP.com/nodvr-live/CiscoTest1/iphone.m3u8",
                "version": "3"
            },
            {
                "type": "hls",
```

```
                "url": "http://live-ca.VMP.com/nodvr-live/CiscoTest1/mac.m3u8",
                "version": "2"
            }
        ],
        "status": {
            "captureStatus": [
                {
                    "captureEngineIp": "11.0.0.207",
                    "state": "CAPTURING"
                }
            ],
            "state": "CAPTURING"
        },
        "statusCallback": {
            "url": "http://am-cep1-live1.VMP.com:7001/v1/dsw/assetNotify"
        },
        "userData": "CiscoTest1"
    }
]
```

AWM Statistics

The AWM provides internal statistics for AssetWorkflow, CaptureEndPoint, and PublishEndPoint. The AWM supports a REST API to get and clear the statistics.

Get Statistics

```
GET /api/awm/stat HTTP/1.1
```

Clear Statistics

```
DELETE /api/awm/stat HTTP/1.1
```

Sample AWM Statistics

```
{
    "assetWfMgr": {
        "awfDeleteAccepted": 0,
        "awfDeleteRejected": 0,
        "awfUpdateAccepted": 1,
        "awfUpdateRejected": 0
    },
    "assetWfs": {
        "nodvr-live": {
            "assetCreateAccepted": 0,
            "assetDeleteAccepted": 0,
            "awfUpdateAccepted": 1,
            "awfUpdateError": 0,
            "awfUpdateSuccess": 1
        }
    },
    "captureEPs": {
        "ce1": {
            "assetCanceled": 0,
            "assetCompleted": 0,
            "assetCreated": 1,
            "assetDeleteFailed": 0,
            "assetDeleted": 0,
            "assetFailed": 0,
            "awfDeleteError": 0,
            "awfDeleteSuccess": 0,
            "awfUpdateError": 0,
            "awfUpdateSuccess": 1
        }
```

```
    },
    "memory": {
        "heapTotal": 71590912,
        "heapUsed": 41873128,
        "rss": 86011904
    },
    "playbackEPs": {
        "pe1": {
            "awfDeleteError": 0,
            "awfDeleteSuccess": 0,
            "awfUpdateError": 0,
            "awfUpdateSuccess": 1
        }
    }
}
```

AWM Error Log

The AWM can log errors and significant events in an error log. You can also use the error log to trace the execution flow when debugging problems. The AWM supports a REST API to set the level of error logging.

Location of the AWM Error Log

```
/var/log/opt/cisco/VMP/errorlog/awm-errorlog.current
```

Control API

```
POST /api/awm/errorlog HTTP/1.1
    { "level": "trace" }
[ errorlog level: "error", "trace", "detail", "default" ]
```

AWM Transaction Log

The AWM provides the following transaction logs:

- AssetWorkflowMgr transaction log—Logs the following:
  - AWM—AWM system events, AssetWorkflow CRUD

  The AssetWorkflowMgr transaction log is located in the /var/log/opt/cisco/VMP/translogs/awm directory.
- Asset transaction log—Logs asset CRUD and asset lookup transactions.

  The Asset transaction log is located in the /var/log/opt/cisco/VMP/translogs/awm-asset directory.

Sample AWM Transaction Log

```
2014-04-22 19:12:32 live-0-1-awm AWM GET /v1/assetWorkflows/undefined 404: not found
2014-04-22 19:12:33 live-0-1-awm AWM espn: asset workflow created, state=INIT
2014-04-22 19:12:33 live-0-1-awm AWM POST /v1/assetWorkflows 202:espn accepted
2014-04-22 19:12:33 live-0-1-awm AWM espn: asset workflow updating, state=UPDATING
2014-04-22 19:12:33 live-0-1-awm AWM espn: asset workflow CEP update done, state=UPDATING,
cepState=UPDATING, pepState=UPDATING
2014-04-22 19:12:34 live-0-1-awm MPEC 11.0.0.221 POST /api/OriginServices/ 201
2014-04-22 19:12:34 live-0-1-awm MPEC 11.0.0.221 POST /api/OriginServices/1184/SEs 204
2014-04-22 19:12:35 live-0-1-awm MPEC 11.0.0.221 POST
/api/OriginServices/1184/ContentProtectKeyProfiles 201
2014-04-22 19:12:35 live-0-1-awm MPEC 11.0.0.221 PUT /api/OriginServices/1184/ODEConfiguration 201
2014-04-22 19:12:36 live-0-1-awm MPEC 11.0.0.221 POST /api/FileMgmt/files;type=302 200
2014-04-22 19:12:36 live-0-1-awm AWM espn: asset workflow PEP update done, state=UPDATING,
cepState=READY, pepState=UPDATING
2014-04-22 19:12:36 live-0-1-awm AWM espn: asset workflow update done, state=READY, cepState=READY,
pepState=READY
2014-04-22 19:12:36 live-0-1-awm AWM GET /v1/assetWorkflows/espn 200
```

```
2014-04-22 19:12:36 live-0-1-awm MCTC POST 0.0.0.0:5001/api/mce/task 200 success,
taskId=L21vcy9zZXJ2aWNlcy9saXZlXzBfMS9hcHBzL2xpdmVfMF8xLXNtY2FwdHVyZWVwLWNlMS90YXNrcy90YXNrLTAwMDAwMDAw
MDU=
2014-04-22 19:12:36 live-0-1-awm AWM espn/CiscoTest1:Asset state changed to PENDING
2014-04-22 19:12:57 live-0-1-awm AWM POST /api/awm/cep/captureEvent/espn/CiscoTest1 204 success,
status=inProgress
2014-04-22 19:12:57 live-0-1-awm AWM espn/CiscoTest1:Asset state changed to CAPTURING
2014-04-22 19:14:10 live-0-1-awm AWM DELETE /v1/assetWorkflows/espn 202 accepted
2014-04-22 19:14:10 live-0-1-awm AWM espn: asset workflow deleting, state=DELETING
2014-04-22 19:14:10 live-0-1-awm AWM espn: delete INIT assets done, count=0, state=DELETING,
cepState=DELETING, pepState=DELETING
2014-04-22 19:14:10 live-0-1-awm MCTC PUT
0.0.0.0:5001/api/mce/task/L21vcy9zZXJ2aWNlcy9saXZlXzBfMS9hcHBzL2xpdmVfMF8xLXNtY2FwdHVyZWVwLWNlMS90YXNrc
y90YXNrLTAwMDAwMDAwMDU= 204 success
2014-04-22 19:14:10 live-0-1-awm AWM POST /api/awm/cep/captureEvent/espn/CiscoTest1 204 success,
status=stopped
2014-04-22 19:14:10 live-0-1-awm MCTC DELETE
0.0.0.0:5001/api/mce/task/L21vcy9zZXJ2aWNlcy9saXZlXzBfMS9hcHBzL2xpdmVfMF8xLXNtY2FwdHVyZWVwLWNlMS90YXNrc
y90YXNrLTAwMDAwMDAwMDU= 204 success
2014-04-22 19:14:10 live-0-1-awm AWM espn: cancel and delete PENDING/CAPTURING assets done, count: 1,
taskDeleteFailed: 0, assetStoreDeleteCount: 1
2014-04-22 19:14:10 live-0-1-awm AWM espn: asset workflow delete from CEP done, state=DELETING,
cepState=DELETED, pepState=DELETING
2014-04-22 19:14:11 live-0-1-awm MPEC 11.0.0.221 DELETE /api/OriginServices/1184 204
2014-04-22 19:14:11 live-0-1-awm MPEC 11.0.0.221 DELETE /api/FileMgmt/files;type=302/1189 200
2014-04-22 19:14:11 live-0-1-awm AWM espn: asset workflow delete from PEP done, state=DELETING,
cepState=DELETED, pepState=DELETED
2014-04-22 19:14:11 live-0-1-awm AWM espn: asset workflow delete done, state=DELETED, cepState=DELETED,
pepState=DELETED
```

Sample AWM-Asset Transaction Log

```
2014-04-22 19:23:26 live-0-1-awm espn/-: GET /v1/assetWorkflows/espn/assets 200:count=0
2014-04-22 19:23:26 live-0-1-awm espn/CiscoTest1: POST /v1/assetWorkflows/espn/assets 201
2014-04-22 19:23:26 live-0-1-awm espn/CiscoTest1: POST http://11.0.0.200:7001/v1/dsw/assetNotify 204:
Asset state PENDING
2014-04-22 19:23:47 live-0-1-awm espn/CiscoTest1: POST http://11.0.0.200:7001/v1/dsw/assetNotify 204:
Asset state CAPTURING
2014-04-22 19:26:04 live-0-1-awm espn/-: GET /v1/assetWorkflows/espn/assets 200:count=1
2014-04-22 19:26:04 live-0-1-awm espn/CiscoTest1: DELETE /v1/assetWorkflows/espn/assets/CiscoTest1 202
2014-04-22 19:26:04 live-0-1-awm espn/CiscoTest1: POST http://11.0.0.200:7001/v1/dsw/assetNotify 204:
Asset state DELETE_COMPLETE
```

AWM Troubleshooting Tips

- AWT Not Enabled—Asset Resolver Problem, page 176
- AWT Instantiation Failed—Bad AWT Configuration, page 176
- AWT Instantiation Failed—MPE Application Failed, page 177
- AWT Instantiation Failed—MCE Application Failed, page 177
- AWT Configuration Update Failed—Bad Configuration, page 178
- AWT Configuration Update Failed—Update to the MPE Failed, page 178
- AWT Configuration Update Failed—Update to the MCE Failed, page 178
- Live Channel Create Failed—Use-API Interface Failed, page 179
- Live Channel Create Failed—Recording Task Create Failed, page 179

- Live Channel Create Failed—Live Recording Failed, page 179
- Live Channel Failed During Capture, page 180
- Live Channel Delete Failed—Use-API Interface Failed, page 180
- Live Channel Delete Failed—Delete Content Task Failed, page 180
- Live Channel Delete Failed—Channel Delete on MCE Failed, page 180
- VOD Asset Create Failed—Use-API Interface Failed, page 181
- VOD Asset Create Failed—Rejected By the AWM Schema, page 181
- VOD Asset Create Failed—Recording Failed on MCE, page 181
- VOD Asset Delete Failed—Delete Content Task Failed, page 182
- VOD Asset Delete Failed—Asset Not Available, page 182

AWT Not Enabled—Asset Resolver Problem

Impact on the End User

The Asset Workflow Template (AWT) creation failed because the asset resolver file could not be uploaded.

Possible Reasons for Problem

Asset resolver file validation failure because of invalid input to the publish template

Error/Event Messages

Examine the /var/log/opt/cisco/VMP/errorlog/awm-errorlog.current.current error log for the reason that the asset resolver file could not be uploaded:

```
04/23/2014 18:29:23.643: (25348)(ERRO)VosmApi.js:1178 ->
{"fileMgmt":{"$":{"uri":"/api/fileMgmt"},"result":[{"$":{"message":"Invalid
File","status":"fail"}}],"error":[{"$":{"message":" ================ Start validating:
/state/cdsmTemp/tempFile5177776065076908517.xml <AssetResolverRules
========================================================= Displaying Only WARNINGS and ERRORS after
1lines ========================================================= ERROR: Parser Error at (line 1, char
466):Attribute 'keyRotationInterval' is not declared for element 'ContentProtectionProfileName' CDS XML
Configuration File: /state/cdsmTemp/tempFile5177776065076908517.xml Total Number of Errors: 1 Total
Number of Warning: 0 CDS XML Configuration File is NOT CORRECT "}}]}}
```

Examine the /var/log/opt/cisco/VMP/translogs/awm/working.log AWM transaction log for the error response that was received during the file upload:

```
2014-04-23 18:29:23 live-0-1-awm MPEC 11.0.0.201 POST /api/FileMgmt/files;type=302 400
```

Resolution/Logs

- In the Asset Publish Template associated with the Asset Workflow Template, fix the configuration issue reported in the AWM error log file

AWT Instantiation Failed—Bad AWT Configuration

Impact on the End User

Instantiation of the AWT failed.

The AssetMgmt Use-API is not published on the DocServer.

Possible Reasons for Problem

The configuration of the service and the AWT in the DocServer is incorrect and is rejected by the AWM schema.

- Mandatory objects or attributes are missing from the AWT configuration.
- One or more of the AWT attributes is configured with an incorrect value.

Error/Event Messages

Examine the AWM error and transaction logs for detailed information about the configuration errors.

Resolution/Logs

1. Disable the AWT.
2. Correct the service and AWT configuration.
3. Enable the AWT.

AWT Instantiation Failed—MPE Application Failed

Impact on the End User

Instantiation of the AWT failed.

The AssetMgmt Use-API is not published on the DocServer.

Possible Reasons for Problem

The MPE application failed, and the AppStatus.nodeStatus is critical.

- The minimum number of MPE-Workers not available.

Error/Event Messages

Examine the transaction logs, and the MPE-AIC error log.

Resolution/Logs

Verify that the MPE-Controller, and the minimum number of MPE-Workers configured in the SLA are available in the VM pool.

Disable and re-enable the AWT.

AWT Instantiation Failed—MCE Application Failed

Impact on the End User

Instantiation of the AWT failed.

The AssetMgmt Use-API is not published on the DocServer.

Possible Reasons for Problem

The MCE application failed, and the AppStatus.nodeStatus is critical.

- The minimum number of MCE-Workers not available.

Error/Event Messages

Examine the MPE-AIC error log.

Resolution/Logs

Verify that the minimum number of MCE-Workers configured in the SLA are available in the VM pool.

Disable and re-enable the AWT.

AWT Configuration Update Failed—Bad Configuration

Impact on the End User

The AWT configuration update failed.

The AssetMgmt Use-API is in **Failed** state.

Possible Reasons for Problem

The update to the AWT configuration is incorrect and is rejected by the AWM schema.

Error/Event Messages

Examine the AWM error and transaction logs for detailed information about the configuration errors.

Resolution/Logs

1. Disable the AWT.
2. Correct the service and AWT configuration.
3. Enable the AWT.

AWT Configuration Update Failed—Update to the MPE Failed

Impact on the End User

The AWT configuration update failed.

The AssetMgmt Use-API is in **Failed** state.

Possible Reasons for Problem

The AWT configuration update to the MPE failed, and the MPE application status is critical.

Error/Event Messages

Examine the AWM and the MPE-AIC error log.

Resolution/Logs

Verify that the MPE application is functioning normally.

Disable and re-enable the AWT.

AWT Configuration Update Failed—Update to the MCE Failed

Impact on the End User

The AWT configuration update failed.

The AssetMgmt Use-API is in **Failed** state.

Possible Reasons for Problem

The AWT configuration update to the MCE failed.

Error/Event Messages

Examine the AWM and MCE-Controller error and transaction logs, and the MCE-AIC error log.

Resolution/Logs

Verify that the MCE application and ZooKeeper are functioning normally.

Disable and re-enable the AWT.

Live Channel Create Failed—Use-API Interface Failed

Impact on the End User

The attempt to create a Live channel failed.

Possible Reasons for Problem

The Live service AssetMgmt Use-API interface failed.

Error/Event Messages

N/A

Resolution/Logs

See the AWT Configuration Update Failed—Bad Configuration, page 178, the AWT Configuration Update Failed—Update to the MPE Failed, page 178, and the AWT Configuration Update Failed—Update to the MCE Failed, page 178.

Live Channel Create Failed—Recording Task Create Failed

Impact on the End User

The attempt to create a Live channel failed.

Possible Reasons for Problem

The attempt to create a recording task on the MCE-TC failed.

Error/Event Messages

N/A

Resolution/Logs

See the Troubleshooting the MCE, page 147.

Live Channel Create Failed—Live Recording Failed

Impact on the End User

The attempt to create a Live channel failed.

Possible Reasons for Problem

A Live recording failed on the MCE.

Error/Event Messages

N/A

Resolution/Logs

See the Troubleshooting the MCE, page 147.

Live Channel Failed During Capture

Impact on the End User
A Live channel failed during capture.

Possible Reasons for Problem
A failure occurred at the MCE.

Error/Event Messages
N/A

Resolution/Logs
See the Troubleshooting the MCE, page 147.

Live Channel Delete Failed—Use-API Interface Failed

Impact on the End User
An attempt to delete a Live channel from the channel lineup failed.

Possible Reasons for Problem
The Live service AssetMgmt Use-API interface failed.

Error/Event Messages
N/A

Resolution/Logs
See the AWT Configuration Update Failed—Bad Configuration, page 178, the AWT Configuration Update Failed—Update to the MPE Failed, page 178, and the AWT Configuration Update Failed—Update to the MCE Failed, page 178.

Live Channel Delete Failed—Delete Content Task Failed

Impact on the End User
An attempt to delete a Live channel from the channel lineup failed.

Possible Reasons for Problem
The delete content task could not be created on the MCE-TC.

Error/Event Messages
N/A

Resolution/Logs
See the Troubleshooting the MCE, page 147.

Live Channel Delete Failed—Channel Delete on MCE Failed

Impact on the End User
An attempt to delete a Live channel from the channel lineup failed.

Possible Reasons for Problem
The attempt to delete the channel on the MCE failed.

Error/Event Messages

N/A

Resolution/Logs

See the Troubleshooting the MCE, page 147.

VOD Asset Create Failed—Use-API Interface Failed

Impact on the End User

An attempt to create a VOD asset failed.

Possible Reasons for Problem

The VOD service AssetMgmt Use-API interface failed.

Error/Event Messages

N/A

Resolution/Logs

See the AWT Configuration Update Failed—Bad Configuration, page 178, the AWT Configuration Update Failed—Update to the MPE Failed, page 178, and the AWT Configuration Update Failed—Update to the MCE Failed, page 178.

VOD Asset Create Failed—Rejected By the AWM Schema

Impact on the End User

An attempt to create a VOD asset failed.

Possible Reasons for Problem

The asset create was rejected by the AWM schema.

Error/Event Messages

The API returns a 400 error code with details in the body.

Resolution/Logs

Correct the asset configuration.

VOD Asset Create Failed—Recording Failed on MCE

Impact on the End User

An attempt to create a VOD asset failed.

Possible Reasons for Problem

The VOD recording failed on the MCE.

Error/Event Messages

N/A

Resolution/Logs

See the Troubleshooting the MCE, page 147.

VOD Asset Delete Failed—Delete Content Task Failed

Impact on the End User

An attempt to create a VOD asset failed.

Possible Reasons for Problem

The delete content task could not be created on the MCE-TC.

Error/Event Messages

N/A

Resolution/Logs

See the Troubleshooting the MCE, page 147.

VOD Asset Delete Failed—Asset Not Available

Impact on the End User

An attempt to create a VOD asset failed.

Possible Reasons for Problem

The asset is not available on the AWM asset store.

Error/Event Messages

The API returns a 404 error code with details in the body.

Resolution/Logs

Examine the workflowId and contentId.

Troubleshooting the Service Instances

- Service Instance Creation, page 182
- Service Instance Update, page 182
- Service Instance Deletion, page 183

Service Instance Creation

The Service Instance Controller (SIC) is spawned by the SICM. The SICs then launch AICs on the same Platform Manager (PM). Processes are not distributed across PMs at startup.

The SICM followers s run on the other PAMs and can take over as leader if the current SICM leader fails. The SICM followers do not launch any SICs or AICs.

Service Instance Update

When there is a VMP configuration change, the DocServer notifies the affected SIC. The SIC then pushes the new configuration to all of its AICs, and each AIC pushes the configuration to its nodes (VMs).

The DocServer notifies the Live or VOD SIC of any configuration changes via callbacks. The SIC then pushes the new configuration to all of its AICs, and each AIC pushes the configuration to its nodes (VMs).

Service Instance Deletion

When a user disables a service via the VMP-M GUI:

1. The DocServer notifies the affected SIC.
2. The SIC posts a **delete** command to each of its AICs.

   The **delete** command does not delete ingest VOD assets are not deleted. To delete ingest VOD assets, use the Service Use API.
3. The AICs are deleted serially: First AWM, then MPE, then MCE. All tasks (live channels) are stopped by the AWM, then the other AICs are deleted.
4. The AICs then post **delete** commands to their workers (VM nodes) and release them back to the PM.
5. All SIC and AIC processes are stopped and the ZooKeeper nodes are cleaned up.

BETA Features

FairPlay Streaming (FPS) is a Beta feature for the 2.8.1 release.

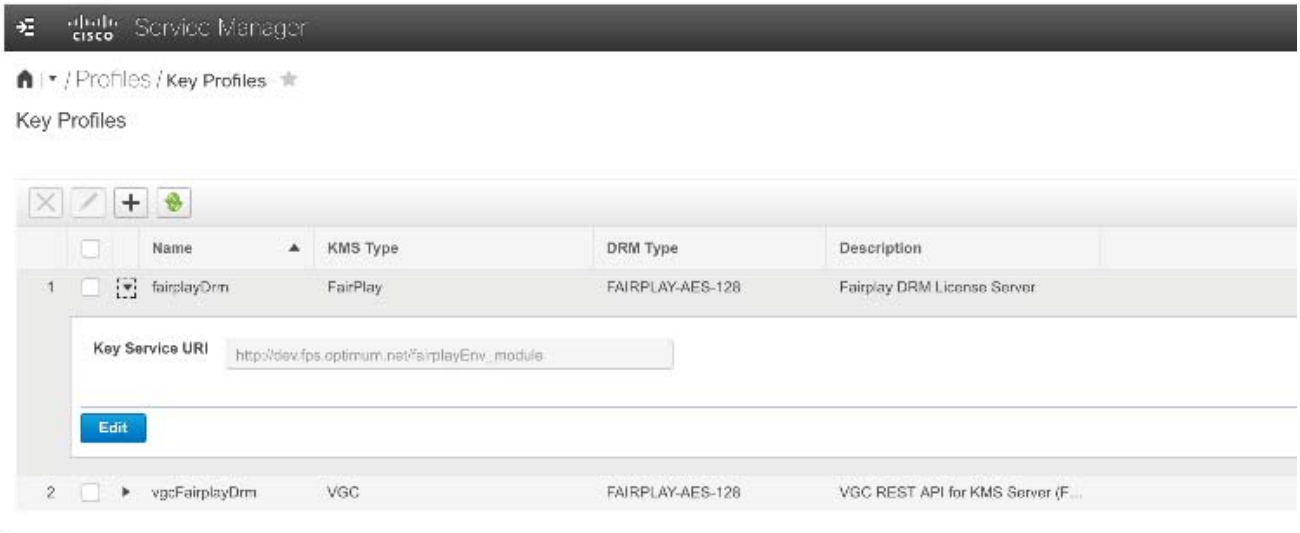
FairPlay Streaming (FPS)

FairPlay Streaming (FPS) technology developed by Apple allows content providers, encoding vendors, and delivery networks to securely deliver keys to Apple mobile devices (iOS), Apple TV (tvOs), and Safari on OS X, which enables playback of encrypted video content. This content is delivered over the web using HTTP Live Streaming (HLS). In this release, Cisco is supporting FPS. For an overview of FairPlay Streaming, refer to https://developer.apple.com/streaming/fps/.

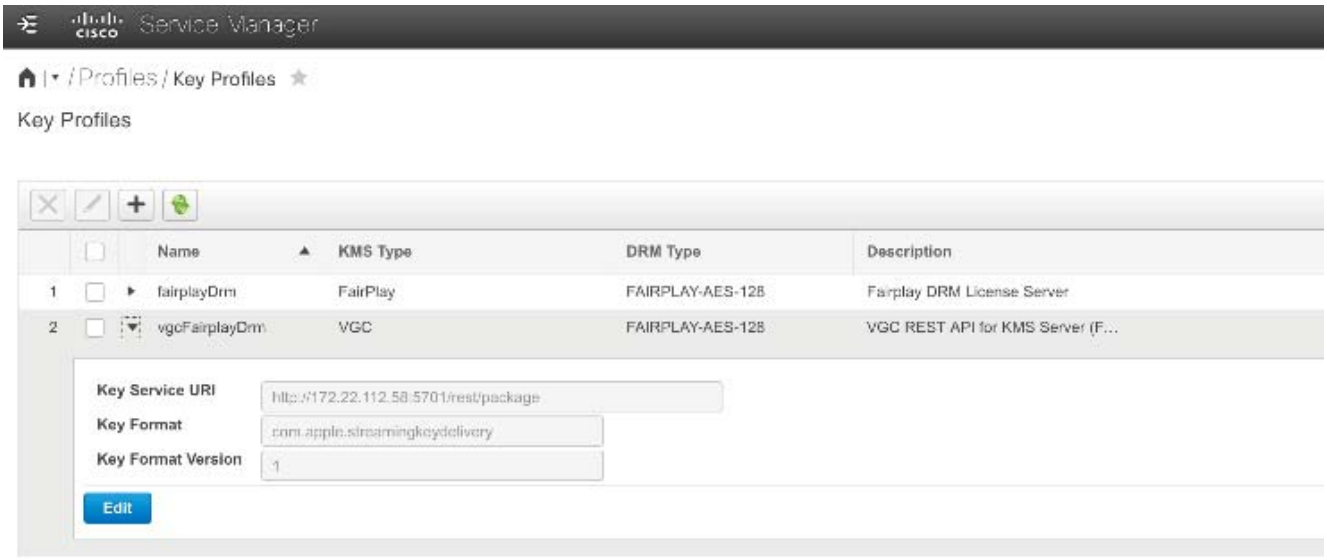
Configuring Key Profiles

Configuring new Key Profiles is required for FPS. The key profiles are configured within the VMP (MPC PAM GUI). The screen shot examples below show key profile configurations.

FairPlay



VGC FairPlay



Adding EXT-X-Key Tag

The VMP component adds a special EXT-X-KEY tag to the .m3u8 file. See examples below.

FairPlay DRM Example:

```
#EXTM3U
#EXT-X-TARGETDURATION:3
#EXT-X-VERSION:5
#EXT-X-MEDIA-SEQUENCE:34
#EXT-X-KEY:METHOD=SAMPLE-AES,KEYFORMAT="com.apple.streamingkeydelivery",KEYFORMATVERSIONS="1",URI="skd:
//CHANFPSAAC",IV=0x67598e96f6ed57ad686bc0568cd0b88c
#EXTINF:2.002,
3400000/6306300.ts
#EXTINF:2.002,
3400000/6486480.ts
#EXTINF:2.002,
3400000/6666660.ts
#EXTINF:2.002,
3400000/6846840.ts
```

VGC FairPlay DRM Example:

```
#EXTM3U
#EXT-X-TARGETDURATION:3
#EXT-X-VERSION:5
#EXT-X-MEDIA-SEQUENCE:0
#EXT-X-PLAYLIST-TYPE:VOD
#EXT-X-KEY:METHOD=SAMPLE-AES,KEYFORMAT="com.apple.streamingkeydelivery",KEYFORMATVERSIONS="1",URI="skd:
//8170150000081041DD2A1DF4119EE03D84859772AC7B1000",IV=0x0913c668a1c7b5d2d0f5b961addf21c8
#EXTINF:2.002,
2100000/4970988298.ts
#EXTINF:2.002,
2100000/4971168478.ts
#EXTINF:2.002,
2100000/4971348658.ts
#EXTINF:2.002,
2100000/4971528838.ts
```

PlayBack

Custom apps are required for playback. The FairPlay iOS app is required for FairPlay DRM and the VGC Multi-DRM app is required for VGC FairPlay DRM

Limitations

- Only H.264 video and AAC audio supported
- FairPlay - Live supported
- VGC FairPlay - Live, VOD, and cDVR supported