Avid MediaCentral Platform Services

Installation and Configuration Guide

Version 2.9

Legal Notices

Product specifications are subject to change without notice and do not represent a commitment on the part of Avid Technology, Inc.

This product is subject to the terms and conditions of a software license agreement provided with the software. The product may only be used in accordance with the license agreement.

This product may be protected by one or more U.S. and non-U.S patents. Details are available at www.avid.com/patents.

This guide is protected by copyright. This guide is for your personal use and may not be reproduced or distributed, in whole or in part, without permission of Avid. Reasonable care has been taken in preparing this guide; however, it may contain omissions, technical inaccuracies, or typographical errors. Avid Technology, Inc. disclaims liability for all losses incurred through the use of this document. Product specifications are subject to change without notice.

The following disclaimer is required by Apple Computer, Inc.:

APPLE COMPUTER, INC. MAKES NO WARRANTIES WHATSOEVER, EITHER EXPRESS OR IMPLIED, REGARDING THIS PRODUCT, INCLUDING WARRANTIES WITH RESPECT TO ITS MERCHANTABILITY OR ITS FITNESS FOR ANY PARTICULAR PURPOSE. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES. THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY PROVIDES YOU WITH SPECIFIC LEGAL RIGHTS. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM STATE TO STATE.

The following disclaimer is required by Sam Leffler and Silicon Graphics, Inc. for the use of their TIFF library:

The following disclaimer is required by the Independent JPEG Group:

This software is based in part on the work of the Independent JPEG Group.

This Software may contain components licensed under the following conditions:

The following disclaimer is required by Paradigm Matrix:

Portions of this software licensed from Paradigm Matrix.

The following disclaimer is required by Ray Sauers Associates, Inc.:

“Install-It” is licensed from Ray Sauers Associates, Inc. End-User is prohibited from taking any action to derive a source code equivalent of “Install-It,” including by reverse assembly or reverse compilation, Ray Sauers Associates, Inc. shall in no event be liable for any damages resulting from reseller’s failure to perform reseller’s obligation; or any damages arising from use or operation of reseller’s products or the software; or any other damages, including but not limited to, incidental, direct, indirect, special or consequential Damages including lost profits, or damages resulting from loss of use or inability to use reseller’s products or the software for any reason including copyright or patent infringement, or lost data, even if Ray Sauers Associates has been advised, knew or should have known of the possibility of such damages.

The following disclaimer is required by Videomedia, Inc.:

“Videomedia, Inc. makes no warranties whatsoever, either express or implied, regarding this product, including warranties with respect to its merchantability or its fitness for any particular purpose.”

“This software contains V-LAN ver. 3.0 Command Protocols which communicate with V-LAN ver. 3.0 products developed by Videomedia, Inc. and V-LAN ver. 3.0 compatible products developed by third parties under license from Videomedia, Inc. Use of this software will allow “frame accurate” editing control of applicable videotape recorder decks, videodisc recorders/players and the like.”

The following disclaimer is required by Altura Software, Inc. for the use of its Mac2Win software and Sample Source Code:

The following disclaimer is required by 3Prong.com Inc.:

Certain waveform and vector monitoring capabilities are provided under a license from 3Prong.com Inc.

The following disclaimer is required by Interplay Entertainment Corp.:

The “Interplay” name is used with the permission of Interplay Entertainment Corp., which bears no responsibility for Avid products.

This product includes portions of the Alloy Look & Feel software from Incors GmbH.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product may include the JCifs library, for which the following notice applies:

Avid Interplay contains components licensed from LavanTech. These components may only be used as part of and in connection with Avid Interplay.

Attn. Government User(s). Restricted Rights Legend

U.S. GOVERNMENT RESTRICTED RIGHTS. This Software and its documentation are “commercial computer software” or “commercial computer software documentation.” In the event that such Software or documentation is acquired by or on behalf of a unit or agency of the U.S. Government, all rights with respect to this Software and documentation are subject to the terms of the License Agreement, pursuant to FAR §12.212(a) and/or DFARS §227.7202-1(a), as applicable.

Trademarks

Avid, the Avid Logo, Avid Everywhere, Avid DNXHD, Avid DNXHR, Avid Nexis, AirSpeed, Eleven, EUCON, Interplay, iNEWS, ISIS, Mbox, MediaCentral, Media Composer, NewsCutter, Pro Tools, ProSet and RealSet, Maestro, PlayMaker, Sibelius, Symphony, and all related product names and logos, are registered or unregistered trademarks of Avid Technology, Inc. in the United States and/or other countries. The Interplay name is used with the permission of the Interplay Entertainment Corp. which bears no responsibility for Avid products. All other trademarks are the property of their respective owners. For a full list of Avid trademarks, see: http://www.avid.com/US/about-avid/legal-notices/trademarks.

Footage

WCAU Fire Story — Courtesy of NBC-10, Philadelphia, PA.

News material provided by WFTV Television Inc.

Avid MediaCentral Platform Services Installation and Configuration Guide • Created March 14, 2017 • This document is distributed by Avid in online (electronic) form only, and is not available for purchase in printed form.

Contents

Using This Guide

This document provides instructions for installing and configuring a new MediaCentral Platform Services (MCS) server or cluster of servers. Avid recommends that you read all the information in the *Avid MediaCentral Platform Services ReadMe* and thoroughly before installing or using the corresponding software release.

If you are completing an installation in a virtual environment, begin the process by referencing the *Avid MediaCentral Platform Services Virtual Environment with VMware® Best Practices Guide*. The virtualization guide directs you back to this guide at the appropriate time in the install process.

To complete an upgrade from a previous version of MediaCentral Platform Services, see the *MediaCentral Platform Services Upgrade Guide* or the *Avid MediaCentral Platform Services ReadMe*.

The following documents are referenced in this guide:

- *Avid MediaCentral Platform Services ReadMe* – Read prior to completing any MCS installation or upgrade
- *MediaCentral Platform Services Concepts and Clustering Guide* – A reference guide that contains more detailed information on systems and topics included in this guide.
- *Avid MediaCentral Platform Services Upgrade Guide* – Reference if you are upgrading to MCS v2.9 from an earlier release
- *Avid Media | Index Configuration Guide* – Reference if configuring Media Index
- *Media |Distribute Installation and Configuration Guide* – Reference if installing Media Distribute
- *Avid MediaCentral | UX Administration Guide* – Contains administrative information for MediaCentral UX.
- *Avid MediaCentral Platform Services Hardware Guide* - Provides detailed information on HP and Dell servers.
- *Avid MediaCentral Platform Services Virtual Environment with VMware® Best Practices Guide* - Provides detailed information on configuring a virtual MCS environment.

Important: See the following link on the Avid Knowledge Base for the latest updates to this guide and all related documentation:

http://avid.force.com/pkb/articles/en_US/readme/Avid-MediaCentral-Version-2-9-x-Documentation

For a list products qualified for use with MCS v2.9, and the supported RHEL operating system, see the Software Compatibility Matrix on the Avid Knowledge Base.

Revision History

Date Revised	Changes Made
March 14, 2017	• Section in Appendix A for “Modifying Configuration Files” has been relocated to the *Avid MediaCentral Platform Services Upgrade Guide*. • Added note to the “Software Installation” chapter regarding a BIOS setting change for HP Gen9 servers that could result in a black display on first boot. • Player demo page should be accessed using a secure “https” address. For more information, see “Enabling the Player Demonstration Web Page” on page 250.
February 16, 2017	• Updated “Installing Security Updates” on page 88 with example output from the avid-security-check script. • Added manual steps to create the cluster resource for the Closed Captioning Service. For details, see “Installing the Closed Captioning Service in a Cluster” on page 168.
February 1, 2017	• Updated Maestro UX install, upgrade and uninstall processes. • Updates to the sharded Mongo configuration process, including: - Windows arbiter running PowerShell v3.0 requires a Windows hotfix - Added processes to disable SELinux and firewall service on a Linux arbiter • Additional step for configuring the permissions of the ntpd file used for time synchronization. For more information, see “Synchronizing the System Clock” on page 80. • Clarification regarding the `cluster setup-cluster` command to specify the use of hostnames with the drbd_exclude option. For more information, see “Starting the Cluster Services on the Master Node” on page 124.
December 22, 2016	Initial v2.9.0 release • Added new chapter, “Assignments Pane” on page 204. • Altered the process for adding a single IP address when Configuring Access for External Systems. • A new script has been created to verify the installation of RHEL security updates. For more information, see “Installing Security Updates” on page 88. • Changes to the sharded Mongo configuration process, including: - Configuration of sharded Mongo for the avid-asset service - Changes to the configuration of the ansible hosts file - Updated output of the `mongo-create-configuration` script, `mongo-checker` script, and other related sharded Mongo scripts For more information see, “Sharded MongoDB” on page 129 and “Working with Sharded Mongo” on page 277. Additional information can be found in the *MediaCentral Platform Services Concepts and Clustering Guide*. • Support for Maestro UX Plug-In with Corosync cluster configurations. For more information, see “Maestro UX Plug-In” on page 184.

Important Terms

Throughout this document, “Avid MediaCentral Platform Services” is referred to as “MCS”. “Red Hat Enterprise Linux” is referred to as “RHEL”.

The RHEL deployment used in an MCS environment is a command-line based operating system. The installation process will require the editing of various system files. Although multiple text editors exist, the tool used throughout this document is “vi”. If needed, a short introduction to vi is included in the *MediaCentral Platform Services Concepts and Clustering Guide*.

⚠ **If copying / pasting commands from this document into a command line interface such as Putty, be sure to verify the command after pasting. It is possible that some characters might be replaced during the paste process which can lead to a failed or problematic installation.**

When working in Linux, this guide assumes the user is logged in as the “root” user. Perform all commands and server configuration as the “root” user.

Technology Previews

This release of MediaCentral Platform Services might contain features that are included as a “Technology Preview”. Features that fall under this category are clearly identified using the Technology Preview terminology. All other features discussed in this document are fully implemented and are not considered as a preview.

What is a Technology Preview?

Avid Technology defines a “Technology Preview” as a feature that is offered to customers for experimentation with the understanding that Avid expects to fully implement the feature in a future release. Technology Preview features are officially unsupported and potentially incomplete or unsuitable for production systems. It is possible that due to unforeseen circumstances, the feature will be altered or altogether removed from the shipping product. In the future, Technology Preview features might be licensed and sold by Avid and use of the feature does not constitute receipt of a permanent license.

Customer feedback regarding the technology preview is welcome. Customers may contact Avid Customer Care to create support cases regarding the feature. However, cases specifically related to the Technology Preview will not be escalated to critical status and might not be resolved.

Symbols and Conventions

Avid documentation uses the following symbols and conventions:

Symbol or Convention	Meaning or Action
📝	A note provides important related information, reminders, recommendations, and strong suggestions.
⚡	A warning describes an action that could cause you physical harm. Follow the guidelines in this document or on the unit itself when handling electrical equipment.

Symbol or Convention	Meaning or Action
⚠	A caution means that a specific action you take could cause harm to your computer or cause you to lose data.
>	This symbol indicates menu commands (and subcommands) in the order you select them. For example, File > Import means to open the File menu and then select the Import command.
▸	This symbol indicates a single-step procedure. Multiple arrows in a list indicate that you perform one of the actions listed.
(Windows), (Windows only), (Macintosh), or (Macintosh only)	This text indicates that the information applies only to the specified operating system, either Windows or Macintosh OS X.
Bold font	Bold font is primarily used in task instructions to identify user interface items and keyboard sequences.
Italic font	Italic font is used to emphasize certain words and to indicate variables.
`Courier Bold font`	Courier Bold font identifies text that you type.
Ctrl+key or mouse action	Press and hold the first key while you press the last key or perform the mouse action. For example, Command+Option+C or Ctrl+drag.

If You Need Help

If you are having trouble using your Avid product:

1. Retry the action, carefully following the instructions given for that task in this guide. It is especially important to check each step of your workflow.
2. Check the latest information that might have become available after the documentation was published. You should always check online for the most up-to-date release notes or ReadMe because the online version is updated whenever new information becomes available. To view these online versions, select ReadMe from the Help menu, or visit the Knowledge Base at http://avid.force.com/pkb/articles/en_US/user_guide/Avid-MediaCentral-Documentation.
3. Check the documentation that came with your Avid application or your hardware for maintenance or hardware-related issues.
4. Visit the online Avid Knowledge Base. Online services are available 24 hours per day, 7 days per week. Search this online Knowledge Base to find answers, to view error messages, to access troubleshooting tips, to download updates, and to read or join online message-board discussions.

Avid Training Services

Avid makes lifelong learning, career advancement, and personal development easy and convenient. Avid understands that the knowledge you need to differentiate yourself is always changing, and Avid continually updates course content and offers new training delivery methods that accommodate your pressured and competitive work environment.

For information on courses/schedules, training centers, certifications, courseware, and books, please visit www.avid.com/support and follow the Training links, or call Avid Sales at 800-949-AVID (800-949-2843).

1 Installation Prerequisites

Chapter Overview

The purpose of this chapter is to guide the preparation of all materials needed for the MCS installation and to preconfigure all connected systems for integration with MCS.

The following table describes the topics covered in this chapter:

Step	Task	Time Est
1	Before You Begin	*varies*
	A quick check to make sure you have everything in place for an efficient and successful installation.	
2	Network Interface Cards and Network Connections	15 min
	Network connection information for various deployment options.	
3	Planning for the Mongo Arbiter	5 min
	In two-node cluster configurations, a 3rd system is required to serve as a Mongo tiebreaker.	
4	Accessing the MCS Server(s)	1 min
	Understanding how to connect to the MCS server(s).	
5	Obtaining the Software	*varies*
	Where to find all the software necessary for the installation.	
6	Copying Software to the MCS Server	*varies*
	This section provides links to processes to copy software to the server.	
7	Updating MediaCentral UX Licenses	15 min
	Licensing requirements for Interplay Production and iNEWS.	
8	Creating User Accounts	10 min
	Covers the creation of user accounts required by MCS.	
9	Adjusting Interplay Production Settings	5 min
	Information on adjusting settings required by MCS.	
10	Verifying Interplay Production Media Indexer Configuration	5 min
	To avoid issues when testing the system, verify that the Media Indexer is configured.	
11	Adding the MediaCentral UX Version to Avid iNEWS	5 min
	Enables MediaCentral UX user to connect to iNEWS.	

Step	Task	Time Est
12	Installing the MediaCentral Distribution Service	10 min
	Required for certain Interplay Production workflows.	
13	Creating the MCS Installation USB Drive	45 min
	In this procedure, you create the USB drive you will use to install the MCS software.	

Before You Begin

A successful MCS installation begins with careful planning. Ensuring that you have identified all prerequisites to the installation is very important. Examples:

- Networking: Define all IP addresses, host names, domain name, DNS, NTP, SNMP, etc.

Hostnames should comply with "RFC 952" and "RFC-1123" standards. Avid recommends keeping host names under 15 characters to maintain backwards compatibility with older systems. The only "special character" allowed in a hostname is a dash " - ". Underscores are not allowed.

For more information on RFC specifications, see https://ietf.org/rfc.html. For additional information on host name restrictions in Microsoft Windows domains, see https://technet.microsoft.com/en-us/library/cc959336.aspx.

- Security and Port usage: Verify that all ports required for your installation are open between switches and across firewalls.

  For more information, see the *Avid Networking Port Usage Guide* on the Avid Knowledge Base.
- Cluster-specific information: Define additional IP addresses, virtual host name and e-mail addresses to be used with the cluster. When defining a virtual host name, make sure to adhere to the "RFC 952" and "RFC-1123" standards.

  For more information see "Clustering" on page 118.
- Users: Identify users, user groups, and passwords (both local and domain users)
- Host Solutions: Identify what systems will connect to MCS. Once identified, it is also important to verify that these systems are available and operating normally. Examples:
  - Avid shared storage (Avid NEXIS, Avid | ISIS)
  - Avid | iNEWS
  - Interplay | Production
  - Interplay | MAM
  - Media Composer | Cloud

  For Interplay | Production deployments, the following systems could also be required:
  - Interplay | Production Services Automation and Interplay | Consolidate (Required for certain Interplay | Delivery workflows. Media | Index is required for this functionality.)
  - Interplay | Transcode (Required for Send To Playback workflows)
  - Interplay | STP Encode (Required for Send To Playback of Long GOP media formats)
  - Interplay | Transfer (Required for Send To Playback to 3rd party playback solutions)

To assist in ensuring you have all the information you need prior to beginning the installation, Avid provides a “Pre-Flight Checklist” available on the Documentation pages of the Avid Knowledge Base. Avid recommends completing the Pre-Flight information to avoid delays during the installation process.

While the installation procedures for MediaCentral UX, Media Composer Cloud and Interplay MAM are very similar, the configuration steps are different. Any configuration differences between MediaCentral UX and Media Composer Cloud will be identified in this document. For differences in the Interplay MAM configuration process, refer to the *Interplay | MAM Installation Manual*.

MCS is available in single server and cluster configurations. A cluster is a group of MCS servers that provide redundancy, load balancing, and scale. Each server in a cluster is called a “node”. During the cluster configuration, one server is identified as the Master node. If you have multiple MCS servers in a rack, the Master node is usually the top-most server in the rack.

If you are configuring a cluster, complete the BIOS and RAID Configuration, Software Installation, and Configuring MediaCentral chapters concurrently on all cluster nodes. The Clustering chapter of this guide must be completed on the Master node only, until otherwise instructed.

Network Interface Cards and Network Connections

Avid supports the on-board 1 Gb NIC for each of the HP DL360 Gen8 / Gen9 and Dell R620/R630 servers. However, certain workflows require the increased bandwidth of an add-in 10 Gb card. For example, a 10 Gb connection is required for any MCS deployment that will use 100+ Mbps video formats (e.g., AVC-I 100, DVCPro 100, DNxHD 145). 10 Gb connections may be desired for additional bandwidth / playback streams

For more information on slot locations, see “Card Placement in MCS Servers” on page 245.

For more information on determining 1 Gb or 10 Gb connections as well as information on supported network adapters, see the *MediaCentral Platform Services Hardware Guide*.

If you plan to configure more than one network adapter on the MCS server, you must manually assign an adapter to RabbitMQ messaging service. For more information, see “Specifying the RabbitMQ Network Adapter” on page 256.

The *Zone* in which the network connection is made must also be considered.

- **Zone 1**: Connected through a 1 Gb or 10 Gb port (direct connect). On an ISIS 7500, this is a direct connection to an ISS switch. On an ISIS 5500, this is a direct connection to the back of the ISIS 5500 chassis.
- **Zone 2**: Connected through a 1 Gb or 10 Gb port on an Avid qualified layer-2 switch (non-routed).
- **Zone 3**: Connected to an Avid qualified layer-3 switch (routed) with known Quality of Service (QoS); traffic routed to Avid shared storage (one hop) and (if applicable) load-balanced across ISIS VLANs (approximately a 60/40 ratio).

All MediaCentral Platform Services servers in a cluster must be in the same subnet.

Zone Recommendations:

MediaCentral UX and Media Composer Cloud

In this workflow MCS decodes the source media format on Avid shared storage and streams images and sound to the clients. This workflow requires MCS to connect to an Avid share storage system.

Zone 1, Zone 2, or Zone 3 (recommended) connections are supported.

Interplay MAM

In this workflow MCS provides playback of video assets registered as browse proxies by Interplay MAM. The connection required depends on where the browse proxies are stored.

For non-Avid storage, the network connection is at the user's discretion as long as it is a 1 Gb connection or better.

For Avid shared storage, Zone 1, Zone 2, or Zone 3 (recommended) connections are supported.

Avid iNEWS

iNEWS-only deployments do not require a connection to a storage system as there is no video playback component. The network connection is at the user's discretion as long as it is a 1 Gb connection or better.

Remote Client Connections

MediaCentral UX web or mobile clients that connect through the public Internet require VPN access into the server network. All connections pass through the VPN router/firewall through identified ports. Once the data has passed into the "house network", it is secured using the customer's existing network security infrastructure.

For more information on networking in an Avid environment, see "Network Requirements for ISIS and Interplay PAM and MAM" located on the Avid Knowledge Base at: http://avid.force.com/pkb/articles/en_US/compatibility/en244197

For information on port usage and network firewall information, see the Avid Networking Port Usage Guide at: http://avid.force.com/pkb/articles/en_US/readme/Avid-Networking-Port-Usage-Guide

Planning for the Mongo Arbiter

MediaCentral v2.6 introduced a new Mongo database in a "sharded" configuration. In MCS cluster and multi-zone configurations, multiple servers host a copy or "shard" of the Mongo database. If you are running a local (non-multi-zone) Corosync cluster that consists of only two nodes, a 3rd instance of Mongo must be configured to provide a tiebreaker vote in the event of a fail-over. This 3rd instance or "arbiter" must be installed on another Linux server or a Windows-based system. If you have a 2-node cluster, plan which system will host the Mongo arbiter.

For more information, see the Sharded MongoDB chapter as well as the "MongoDB" section of the *MediaCentral Platform Services Concepts and Clustering Guide*.

If you are running a single-server, non-multi-zone system, no additional configuration steps for sharded Mongo are required.

Accessing the MCS Server(s)

The initial configuration of the MCS server(s) must be completed using a directly connected monitor and keyboard to the server, or through a KVM (keyboard, video and mouse) device.

Some KVMs present virtual USB devices to the operating system. These devices might be assigned a device name (sda, sdb) by RHEL during the installation, which results in a failed installation. Disable this option on your KVM if applicable

Once the initial configuration is complete, Avid recommends connecting to MCS indirectly through SSH (Secure Shell). SSH is preferable for the following reasons:

- Allows for an expandable view of the RHEL interface (adjustable window size)
- Allows for multiple sessions to the host server or to multiple servers
- Allows for simplified copy/paste of commands between SSH windows
- Allows for logging of all session output

On Windows, PuTTY.exe is an example of a SSH client: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

At the appropriate point in the installation procedure, you will be given the option to switch from a direct connection to an indirect connection.

Obtaining the Software

Multiple software packages are required to properly install and configure MCS. These include:

- Red Hat Enterprise Linux (RHEL)
- RHEL Security Updates
- MCS Installation Packages
  - MediaCentral Platform Services
  - (if applicable) MediaCentral Platform Services Updates
  - (if applicable) MediaCentral UX Closed Captioning Service
  - (if applicable) MediaCentral Customizable Logger
  - (if applicable) MediaCentral Distribution Service (MCDS)
  - (if applicable) Interplay MAM Connector
  - (if applicable) Media Composer Cloud Plug-In
  - (if applicable) Media Distribute
  - (if applicable) Maestro UX Plug-In
- GlusterFS
- (if applicable) Storage Controller Driver for the HP ProLiant Gen9 Server

Red Hat Enterprise Linux (RHEL)

Due to licensing restrictions, Avid is unable to redistribute the RHEL installation media. The RHEL installation image (.iso) file can be located at: http://www.redhat.com/en

Log in to your Red Hat Network account and download the DVD image (.iso) file.

At the time of this document's publication, the RHEL 6.5 ISOs were available by choosing Red Hat Enterprise Linux Server from the Red Hat Product Downloads page. Specify Red Hat Enterprise Linux Server (product variant), 6.5 (version) and x86_64 (architecture). Download the Binary DVD (rhel-server-6.5-x86_64-dvd.iso).

MCS requires RHEL 6.5. Do not install any OS updates or patches unless specifically directed to do so by Avid.

RHEL Security Updates

Red Hat has issued various security advisories for RHEL 6.5. Avid has tested and supports the installation of specific patches for RHEL. For instructions and software download links, see the "Security Updates" section in the *Avid MediaCentral Platform Services ReadMe*.

MCS Installation Packages

The MCS software packages are available from the Avid Download Center.

If you have not already created an Avid.com user account, you will need to do so now. This Master Account enables you to sync your Avid Video Download and Avid Video Community accounts as well as gain access to the Avid Support Center.

After you have logged into the Download Center, download the following:

- Avid MediaCentral Platform Services

  This is the primary MCS installer package. All MCS installations will require this software.

- (if applicable) Avid MediaCentral Platform Services Updates

  Avid will often release updates to MCS providing fixes and new features. Consult the ReadMe for your version of software for patch availability and specific installation instructions.

- (if applicable) Avid MediaCentral UX Closed Captioning Service

  Introduced with MCS v2.3, this service adds functionality to MediaCentral UX that enables new closed captioning workflows.

- (if applicable) Avid MediaCentral Customizable Logger

  Introduced with MCS v2.7, these services add functionality to MediaCentral UX that enable enhanced logging workflows.

- (if applicable) MediaCentral Distribution Service (MCDS)

  MCDS is a service that resides on a Windows system that coordinates jobs with Avid Production Services for send-to-playback operations. If your installation will include a STP workflow, download this software.

- (if applicable) Interplay MAM Connector

  The MAM Connector enables Interplay MAM workflows within MediaCentral UX. If your installation includes MAM integration, download this software.

- (If applicable) Media Composer Cloud Plug-In

  The Media Composer Cloud software is a plug-in for the Media Composer editor that enables remote editing capabilities. If your installation includes a Cloud workflow, download this software.

- (If applicable) Media Distribute

  Media Distribute links production with distribution to web, mobile, and social media outlets by orchestrating workflow and automating file preparation and transcoding. Media Distribute is not publicly available on the Avid Download Center at this time. If your installation includes a Distribute workflow, contact your Avid representative for this software.

- (If applicable) Maestro UX Plug-In

  The Maestro UX plug-in enables a connection to the Maestro Asset database for integration with Avid iNEWS and Interplay MAM workflows.

If any of these packages are not available through the Download Center, contact your Avid representative to obtain the necessary software.

GlusterFS

GlusterFS is an open source software package that MCS uses to automate replication of the dedicated media cache volumes (e.g. RAID 5) across all MCS servers in the cluster. Doing so increases the speed at which clients can access the media on multiple cluster nodes.

MediaCentral Platform Services v2.4.0 and later automatically installs the GlusterFS software as part of the install (or upgrade) process. If you are deploying a clustered system, a separate download and installation of the Gluster software is no longer required. If you are deploying a single server configuration, the Gluster software is still installed on the server, but it is not activated or configured.

Storage Controller Driver for the HP ProLiant Gen9 Server

By default the HP ProLiant Gen9 server storage controller does not support RHEL 6.5. Manually download the following RHEL driver update disk (.iso) to enable RHEL 6.5 support:

```
dd-hpsa-18216-x86_64.iso
```

The driver update disk is available directly from Red Hat, but driver details and a link to the correct page can be found at the “HP Servers Support & Certification Matrices” technical exceptions page: http://h17007.www1.hp.com/us/en/enterprise/servers/supportmatrix/exceptions/rhel_exceptions.aspx

This procedure applies to the HP ProLiant Gen9 server only.

To download the driver disk:

1. Open a web browser and navigate to the “HP Servers Support & Certification Matrices technical exceptions page.
2. Locate the link to Red Hat by searching for the words “DL360 Gen9” using the browser’s “find on this page” feature.
3. Click on the RHEL6.5 x86_64 link.

   You are redirected to the Red Hat web site.
4. Log in to your Red Hat Network account.

5. On the “Download Red Hat Enterprise Linux” page, locate the driver update disk (.iso):

   dd-hpsa-18216-x86_64.iso

6. Click the “Download Now” button and save the ISO file to your computer.

   You will use this driver update disk ISO file later when you create the MCS Installation USB drive.

Copying Software to the MCS Server

At various times during the upgrade, you will need to copy software to the MCS server. This task can be performed using one of two methods:

- Using an SFTP application on an external system
- Connecting a USB drive directly to the server

While the SFTP method may be preferred for ease of access, the USB method may be required for some operations such as backing up MCS files during a system upgrade.

For details on each of these methods, see “Copying Software to the MCS Server” on page 238.

Updating MediaCentral UX Licenses

Depending upon your deployment, one or more connected systems may need licenses installed or updated to allow for integration with MCS.

- If connecting to Interplay Production, MediaCentral UX users will consume Interplay Client licenses.
- If connecting to iNEWS, MediaCentral UX users will consume iNEWS Client licenses.
- If connecting to Interplay Production and iNEWS, MediaCentral UX users will consume both Interplay and iNEWS Client licenses.

Interplay Production Licensing

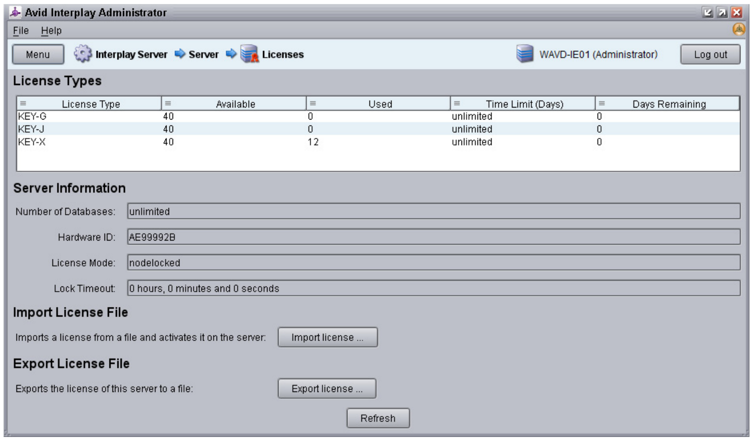
When integrating with an Interplay Production system, MediaCentral UX validates client licenses against the Interplay Engine. New MediaCentral systems are often bundled with additional client licenses which must be added to the Interplay Engine database.

Interplay Production v3.3 introduced a software licensing option (no dongle). The following process is correct for the original dongle licensing process. For software licensing procedures, see the Interplay | Production Software Installation and Configuration Guide.

To add licenses to the Interplay Production Engine:

1. Launch the Interplay Administrator on the Interplay Engine. This can be found at: Start > Avid > Avid Interplay Access Utilities > Avid Interplay Administrator.
2. Sign in using Interplay Production’s Administrator credentials.

3. From the main menu, select Server > Licenses.



License Types

License Type	Available	Used	Time Limit (Days)	Days Remaining
KEY-G	40	0	unlimited	0
KEY-J	40	0	unlimited	0
KEY-X	40	12	unlimited	0

Server Information

Number of Databases: unlimited

Hardware ID: AE99992B

License Mode: nodelocked

Lock Timeout: 0 hours, 0 minutes and 0 seconds

Import License File

Imports a license from a file and activates it on the server: Import license ...

Export License File

Exports the license of this server to a file: Export license ...

4. Click the Import License button.
5. Navigate to the location of the license file (often provided on a USB drive).
6. Select the license file and click Open.

   You should receive a message indicating that the license was successfully activated.
7. Log out of the Interplay Administrator and close the application.

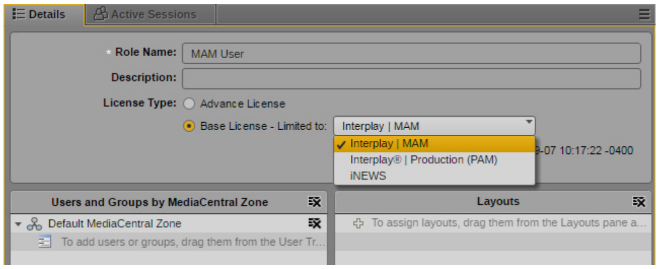
For additional information on the Interplay Administrator, see the I*nterplay | Engine and Interplay | Archive Engine Administration Guide*.

iNEWS Licensing

When integrating with an Avid iNEWS system, MediaCentral UX validates client licenses against the iNEWS server(s). New MediaCentral systems are often bundled with additional client licenses which must be added to the Avid iNEWS database. For more information on adding licenses to the iNEWS database, see "Avid iNEWS Integration" on page 273.

Interplay MAM Licensing

In Interplay Production and iNEWS workflows, users sign into MediaCentral UX and a license is verified with one or both of the back-end systems. In Interplay MAM workflows, MediaCentral UX users use a different licensing process. The system administrator assigns users to a MAM-only role (associated with a base license by default) through the MediaCentral UX User layout. This grants the user access to the Layouts associated with Interplay MAM.



* Role Name: MAM User

Description:

License Type: ○ Advance License

● Base License - Limited to: Interplay | MAM

✓ Interplay | MAM
Interplay® | Production (PAM)
iNEWS
-07 10:17:22 -0400
Users and Groups by MediaCentral Zone
Default MediaCentral Zone
To add users or groups, drag them from the User Tr...
Layouts
To assign layouts, drag them from the Layouts pane a...

Creating User Accounts

This section will cover the creation of user accounts for use with:

- Interplay Production User
- Avid Shared Storage User
- Avid iNEWS User
- Interplay MAM User
- Media Composer Cloud User

Create any user accounts applicable to your installation.

Interplay Production User

When integrating with Interplay Production, MediaCentral UX requires credentials to access the Interplay Production database. This user should have Read/Write privileges to the entire database (at minimum). For consistency purposes, this user and password should be the same as the user you create on the Avid shared system.

Decide upon the name and password for this user now. Suggested user name: **MCSAdmin**

To create the Interplay Production user:

1. Launch the Interplay Administrator on the Interplay Engine. This can be found at: Start > Avid > Avid Interplay Access Utilities > Avid Interplay Administrator.
2. Sign in using Interplay Production's Administrator credentials.
3. From the main menu, select User Management > User Management.
4. If multiple User Groups are created, highlight the User Group on the left under which you want to create your new user. Example: Administrators
5. Click the Create User button at the top of the window.
6. Enter a name and password.
7. Verify that the MediaCentral UX Admin user has at least Read/Write access to the entire database. Administrator-level access is not required, but recommended.
8. Click Apply.
9. Log out of the Interplay Administrator and close the application.

For additional information on users creation in Interplay Production, see the *Interplay | Engine and Interplay | Archive Engine Administration Guide*.

Avid Shared Storage User

When integrating with Interplay Production, MediaCentral UX requires credentials to access the media on the Avid shared storage system to enable playback and allow for the creation of voice-over media. For consistency purposes, this user and password should be the same as the user you create on the Interplay Production system.

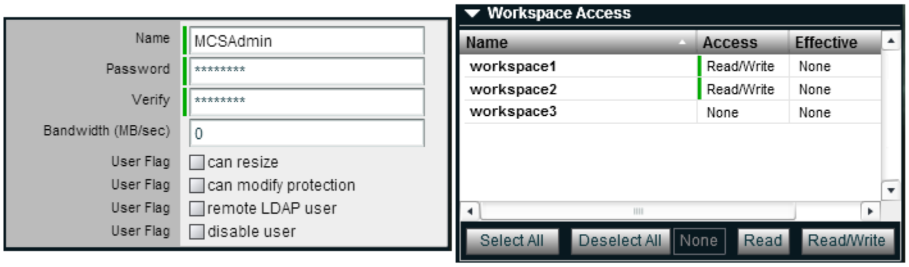
Decide upon the name and password for this user now. Suggested user name: **MCSAdmin**

To create the Avid shared storage user:

1. Launch the Management Console page by opening a web browser and navigating to one of the following:
   - Avid NEXIS: http://<*System Director hostname*>
   - ISIS 2500 or ISIS 5500: http://<*System Director hostname*>
   - ISIS 7500: https://<*System Director hostname*>:5015

In a fail-over configuration, use the virtual System Director hostname. Alternatively, the IP address of the System Director (or virtual System Director) can also be used.

2. Sign in using the Administrator credentials.
3. From the main menu, select System > Users.
4. Click the New button to create a new user.
5. Give the user a Name and Password.



Name	MCSAdmin
Password	********
Verify	********
Bandwidth (MB/sec)	0
User Flag	□ can resize
User Flag	□ can modify protection
User Flag	□ remote LDAP user
User Flag	□ disable user

Workspace Access

Name	Access	Effective
workspace1	Read/Write	None
workspace2	Read/Write	None
workspace3	None	None

The above image taken from the Management Console of an Avid ISIS system. Avid NEXIS does not include the option to Modify Protection.

6. Under Workspace Access, assign privileges to all indexed workspaces. At minimum, the user needs Read access to all workspaces indexed by the Interplay Media Indexer and Read/Write access to the workspace where voice-overs will be recorded (workspace defined in the Interplay Administrator> Application Database Settings).
7. Click Apply to create the user account.
8. Close the Management Console.

If you are connecting to multiple Avid shared storage systems, ensure the same user/password is created on each system.

For additional information on users creation in Interplay Production, see the *Avid NEXIS Administration Guide* or *Avid | ISIS Administration Guide*.

Avid iNEWS User

When integrating with iNEWS, the MCS Administrator requires access to the iNEWS database. This can be accomplished by creating a custom user account (superuser rights not required) or by associating the Administrator with an existing iNEWS account.

Decide upon the name and password for this user now. Suggested user name: **MCSAdmin**

For instructions on creating a custom iNEWS user account for MediaCentral UX, see the *Avid iNEWS Setup and Configuration Guide*.

Interplay MAM User

If you are integrating with MCS as a player for an Interplay MAM system, a specialized user must be created within the MCS user database.

Decide upon the name of this custom user now. Suggested user name: **MAMuser**

For details on creating this user, see "Configuring MCS for Interplay MAM" on page 112.

When installing Interplay MAM, a special user account is created for the MAM Control Center. The user must be a member of the "MAM Administrators" group for MAM Control Center. This means you must have a Windows account on Interplay MAM side that is in your Windows "MAM Administrators" group which can be used by MediaCentral for the MAM connection. If you plan to install the MAM Connector software for MediaCentral UX, the MAM Control Center credentials are used in the System Settings.

For details on the MAM Connector System Settings, see "MAM Connector" on page 211.

For more information on this user and setting, see the *Avid MediaCentral | UX Administration Guide*.

Media Composer Cloud User

When integrating with Media Composer Cloud, you must create a custom user account in the Interplay Administrator ("MediaCentral Platform Services Settings" or "Application Database Settings" in v3.5 and earlier) and in the MediaCentral UX System Settings (MCPS > Player tab). The user name and password must match in both locations.

When added to the MediaCentral UX System Settings, this account is automatically added as an MCS user and assigned a special "Playback-Only Client" user role. This will appear in the Users Layout under Users > Unassigned > Playback-Only.

Rules regarding the specialized user account:

- This must be a unique user created solely for this purpose. Do not use the same user you created to sign into Interplay Production or Avid shared storage.
- Do not use an account that already exists as a Central User. It must be a new user.
- This user should not be created as an Interplay Production or an shared storage user.
- Remember that MCS runs on Linux. Both passwords and user accounts are case sensitive.

Decide upon the name of this custom user now. Suggested user name: **cloud**

For more information, see the *Media Composer | Cloud Installation and Configuration Guide*.

Adjusting Interplay Production Settings

When integrating with Interplay Production, MCS checks with the Interplay Production Engine for various settings. This section is particularly important for sites requiring STP workflows or integrations with Media Composer Cloud.

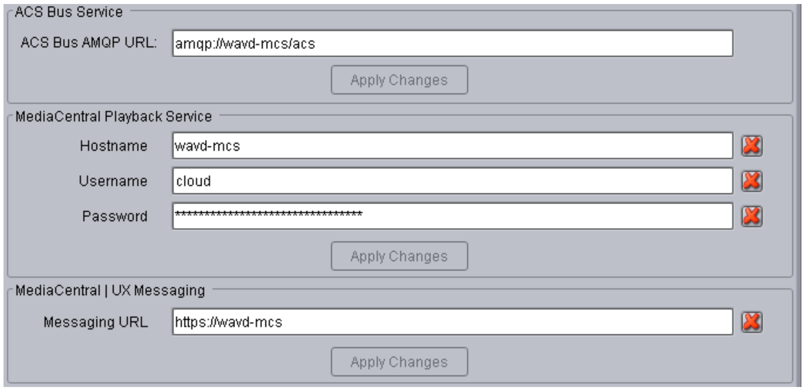
Avid supports configuring one Avid MediaCentral Platform Services system (single-server or cluster) with one Avid Interplay Production database. Configuring multiple MediaCentral systems to connect to a single Interplay Production database is not supported. To connect multiple instances of MediaCentral and Interplay Production together, configure the MediaCentral system for a multi-zone environment. For more information on configuring multi-zone, see the chapter for "Multi-Zone" on page 221.

To configure the Interplay Production settings:

1. Launch the Interplay Administrator on the Interplay Engine. This can be found at: Start > Avid > Avid Interplay Access Utilities > Avid Interplay Administrator
2. Sign in using Interplay Production's Administrator credentials.
3. From the main menu, select Application Settings > Application Database Settings and adjust the following:

   a. Format – Video Format: This setting determines the default video format for sequences created in MediaCentral UX. You must select a specific video format from the menu or leave the default selection of "Any". If "Any" is selected, MediaCentral UX determines the video format of the sequence by using the format of the first clip that the user adds to the timeline.

   b. Audio – General Settings: Ensure that a Media Creation Workspace has been assigned. If this value is empty, voice-over recording in MediaCentral UX will fail.
4. Click Apply.
5. From the main menu, select Site Settings > MediaCentral Platform Services Settings.



ACS Bus Service

ACS Bus AMQP URL: amqp://wavd-mcs/acs

MediaCentral Playback Service

Hostname: wavd-mcs

Username: cloud

Password: ********************************

MediaCentral | UX Messaging

Messaging URL: https://wavd-mcs

In versions of Interplay Production v3.5 and earlier, these settings are located under the Application Database Settings category.

Configure the following settings as they apply to your installation:

a. ACS Bus Service: This feature is used in conjunction with Media Index configurations. For more information, see the *Avid Media | Index Configuration Guide*.

b. MediaCentral Playback Service (Cloud workflow only):

- Hostname: Enter the host name of the MCS server. In the case of a cluster, enter the virtual host name assigned to the cluster.

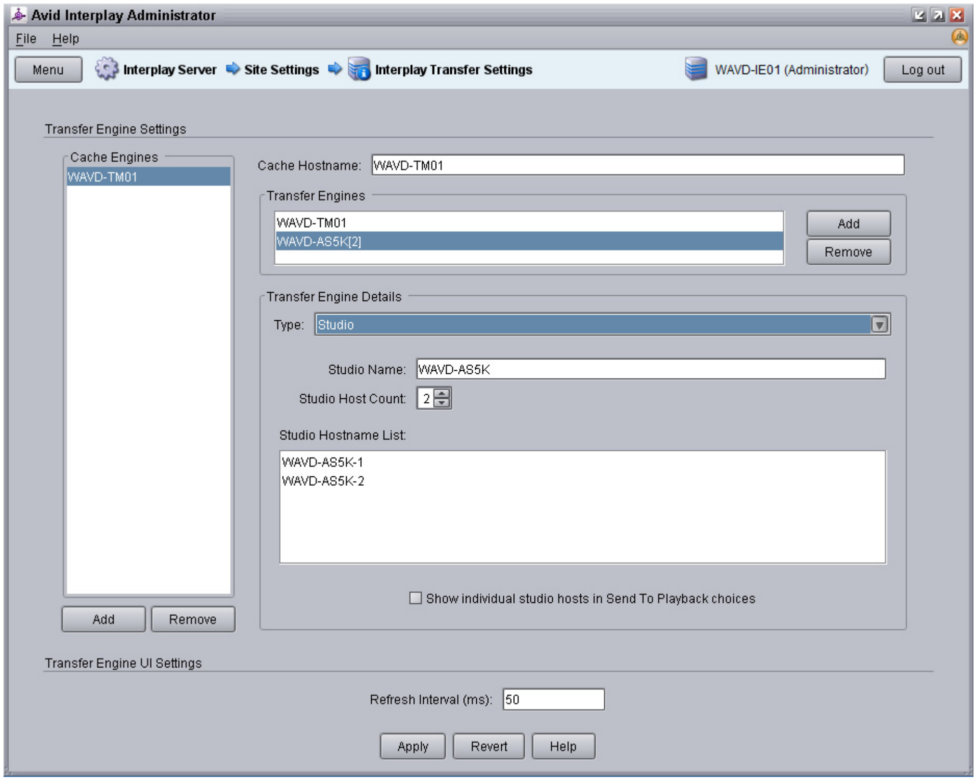
- Username / Password: Specify a custom user name and password that will be used to connect Cloud users to the MediaCentral UX player. This same user / password must be entered in the MediaCentral UX System Settings under the MCPS > Player tab. This must be a unique user created solely for this purpose.

c. MediaCentral | UX Messaging: This setting enables a messaging workflow between MediaCentral UX and Media Composer. Enter the host name of the MCS server in the form of a URL. In the case of a cluster, enter the virtual host name assigned to the cluster.

6. Click the Apply Changes button for any settings that were adjusted.

7. If you are integrating with Media Composer Cloud, you should also configure the Application Settings > Media Composer | Cloud Settings. See the *Media Composer | Cloud Installation and Configuration Guide* for additional details.

8. From the main menu, select Site Settings > Interplay Transfer Settings. MediaCentral polls this setting for available Transfer Engines and AirSpeed servers when creating STP profiles.



Transfer Engine Settings

Cache Engines: WAVD-TM01

Cache Hostname: WAVD-TM01

Transfer Engines:
WAVD-TM01
WAVD-AS5K[2]

Transfer Engine Details

Type: Studio

Studio Name: WAVD-AS5K

Studio Host Count: 2

Studio Hostname List:
WAVD-AS5K-1
WAVD-AS5K-2

□ Show individual studio hosts in Send To Playback choices

Transfer Engine UI Settings

Refresh Interval (ms): 50

9. Click Apply.

Verifying Interplay Production Media Indexer Configuration

MCS v2.5 and later obtains the Media Indexer configuration information directly from the “Server Hostname Settings” in the Interplay Administrator tool. Ensure that the “MI Connection URL” is populated with all Interplay Media Indexer servers and that “Check Media Indexer” returns with no errors. If the settings have not been configured correctly, MediaCentral UX will not be able to load or play assets from Interplay Production. Dynamic Relink functionality within MediaCentral also depends on this setting.

For more information on configuring the Server Hostname Settings, see “Setting Server Hostnames and the Workgroup Name” in the *Interplay Engine and Interplay Archive Engine Administration Guide*.

Adding the MediaCentral UX Version to Avid iNEWS

Before connecting MediaCentral UX to iNEWS, the MediaCentral UX Client version must be added to the iNEWS SYSTEM.CLIENT.VERSIONS file.

Refer to the *Avid MediaCentral Platform Services ReadMe* for the correct version number for your installation.

See the Avid iNEWS Integration chapter for instructions on adding the version number to iNEWS.

Installing the MediaCentral Distribution Service

The MediaCentral Distribution Service (MCDS) is a lightweight application required for Send to Playback (STP) operations. It analyzes the STP request and determines if additional actions are required before sending the media to the playback device (AirSpeed, Transfer Engine, other). An Interplay Transcode provider is required for STP operations requiring audio mixdowns (stereo audio tracks) or video mixdowns (sequences with dissolves). An Interplay STP Encode provider is required when using Long GOP media. For more information on workflows that include MCDS, see the *Avid Interplay Engine and Avid Interplay Archive Engine Administration Guide*.

MCDS is not used if you are sending an asset directly to Transcode or Delivery. MCDS is not used in iNEWS-only configurations.

The following guidelines apply to installing MCDS:

- Supported on Windows 7 64-bit and Windows Server 2012.
  - If you are running Windows Server 2012, you must install the Windows Desktop Experience feature. For more information and installation procedures, see the *Interplay Production Dell and HP Server Support* guide on the Avid Knowledge Base.
  - If you are running Windows 7 N, Windows Media Player must be manually installed. For more information on “N” versions of Windows, see: http://windows.microsoft.com/en-us/windows7/products/what-is-windows-7-n-edition
- Requires a minimum of 512MB of RAM and approximately 380MB of hard drive space on the host server.

- Ensure that all enabled network adapters on both the system hosting the MCDS and the Interplay Production Services Engine are fully routable to each other.
- Can be installed on a server hosting other services or applications, such as the Interplay Production Services Engine, Interplay Transcode, Interplay Transfer Engine, etc.
- Must be installed on a system that has the Avid shared storage client software installed.
- Must not be installed on an Interplay Production Engine or Interplay Archive Engine.
- As of Interplay Production 3.2, MCDS should not be installed on a Media Indexer server as the two systems risk sharing network port 8443.

For redundancy purposes, MCDS can be installed on two systems. Installing a second instance of MCDS does not provide load-balancing functionality. You will configure MediaCentral UX to find the installed instance(s) of MCDS later in this document.

In MediaCentral UX 1.x, the MCDS service used port 8080 for normal http communication. In MediaCentral UX v2.0 / MCDS v3.1, the port changed to 8890. This change allows MCDS to be installed on the same server as the Production Services Engine (if desired). Port 8443 is used for http security protocol.

Versions of MCDS prior to v3.3 required the Interplay Service Framework (32 or 64bit) software to be installed on the system hosting MCDS. As of v3.3, this is no longer a requirement.

MCDS v3.3 and earlier cannot be installed on Interplay Production Transcode or STP Encode servers. This limitation no longer applies to MCDS v3.4 and later.

For additional information on MCDS version compatibility, see the Avid Knowledge Base: http://avid.force.com/pkb/articles/en_US/compatibility/Avid-Video-Compatibility-Charts

To install the MediaCentral Distribution Service:

1. Launch the MCDS installer on your desired system.
2. Proceed through the installation and accept the defaults.

   You may be asked to install prerequisite requirements such as Microsoft Visual C++.
3. Once the installation is complete, use Windows Computer Management to verify that the “Avid Interplay Central Distribution Service” is “Started” and the Startup Type is configured as “Automatic”.
4. If desired, repeat the process on a second system to create a redundant instance of the service.

Creating the MCS Installation USB Drive

The MCS installation is initiated from a bootable USB drive that contains the OS (Red Hat Enterprise Linux) and the MCS software. The following are required to complete this procedure:

- A Windows-based computer
- The MCS installation package (MediaCentral_Services_<*version*>_Linux.zip)
- RHEL installation image (.iso) file
- A 16GB or larger USB drive

Avid has been informed of problems using USB drives from some vendors. If the server does not boot from the USB drive, or fails to complete the boot, try using a drive from another vendor or a drive with a larger capacity (32GB).

The BIOS on some systems do not recognize USB 3.0 drives correctly which results in the inability to boot from them. Avid recommends using a USB 2.0 drive for this process.

This procedure uses an application called “ISO to USB” to create a bootable USB drive containing the required RHEL operating system and MCS files. Do not simply drag and drop installation files onto the USB drive as this will not create the correct file structure needed to successfully install MCS.

Since “ISO to USB” creates a bootable drive, Avid recommends only connecting the USB drive you plan to use to the Windows system. If you have more than one USB drive connected to the system, make sure you choose the correct drive when performing this procedure.

See one of the following two processes, depending on your hardware platform:

- “Preparing the Installation Drive for the HP ProLiant Gen9” on page 33
- “Preparing the Installation Drive for HP Gen8 and Dell Servers” on page 35

Preparing the Installation Drive for the HP ProLiant Gen9

The procedure for creating the MCS installation drive on a ProLiant Gen9 server differs from that of other installations. Make sure you follow the customized instructions for your server type.

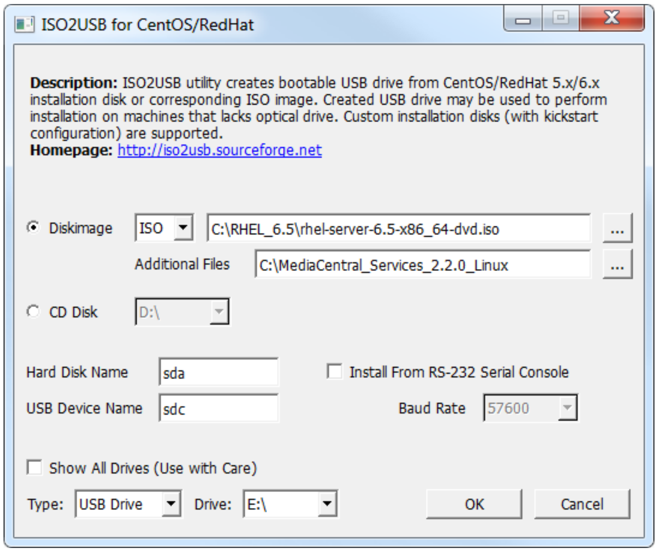
This section contains three procedures:

- Preparing the MCS Installation USB Drive
- Copying the Storage Controller Driver to the USB Drive

To prepare the MCS Installation USB Drive:

1. Sign into a Windows system.
2. Connect the USB drive to the Windows system and give it a few moments to be recognized.
3. Use Windows Disk Management to format the USB drive as a FAT32 volume.
4. Extract the contents of the MediaCentral_Services_<*version*>_Linux.zip file to the desktop (or your preferred destination directory).
5. Open the newly created MediaCentral_Services_<*version*>_Linux folder.

6. Double-click iso2usb.exe to launch the application.



ISO2USB for CentOS/RedHat

Description: ISO2USB utility creates bootable USB drive from CentOS/RedHat 5.x/6.x installation disk or corresponding ISO image. Created USB drive may be used to perform installation on machines that lacks optical drive. Custom installation disks (with kickstart configuration) are supported.
Homepage: http://iso2usb.sourceforge.net

● Diskimage ISO C:\RHEL_6.5\rhel-server-6.5-x86_64-dvd.iso

Additional Files C:\MediaCentral_Services_2.2.0_Linux

○ CD Disk D:\

Hard Disk Name sda

USB Device Name sdc

□ Install From RS-232 Serial Console

Baud Rate 57600

□ Show All Drives (Use with Care)

Type: USB Drive Drive: E:\

7. Choose the Diskimage radio button then navigate to the RHEL image (.iso) file (named rhel-server-6.5-x86_64-dvd.iso or similar).

Make sure the RHEL image (.iso) file is accessible locally (preferable) or over the network from your computer.

8. In the “Additional Files” field, navigate to the MediaCentral_Services_<*version*>_Linux **folder** and click the “Select Folder” button.

9. Use the table below to verify that the Hard Disk Name and USB Device Name fields are correct for your deployment.

RAID Configuration	RAID 1 (“Hard Disk Name”)	RAID 5	USB (“USB Device Name”)
RAID 1 and RAID 5	sda	sdb	sdc
RAID 1 only	sda		sdb

For example, for a system deploying both RAID 1 and RAID 5 volumes, enter the following values in the dialog:

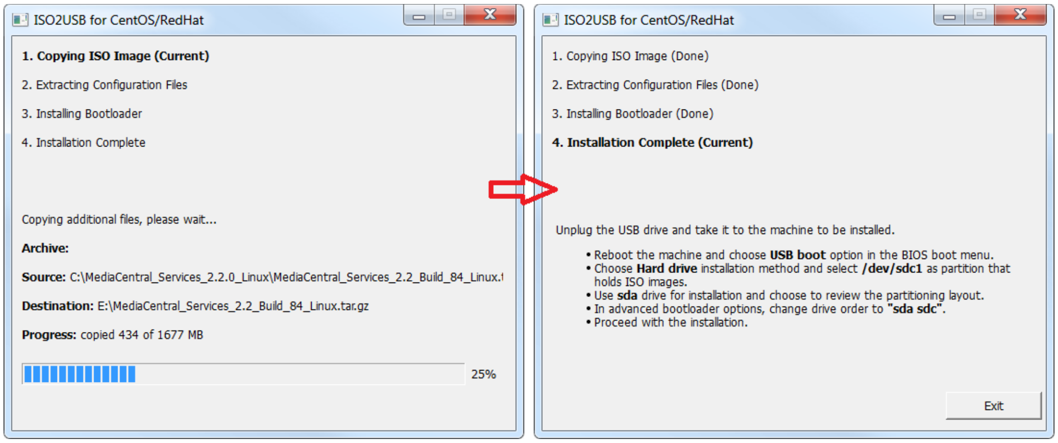
- Hard Disk Name: sda
- USB Device Name: sdc

For those familiar with earlier HP servers, the HP ProLiant Gen9 server identifies the RAID 1, RAID 5, and the USB drive with different device names.

If the drive names are not configured properly in the kickstart file, you could encounter errors in the deployment process. Example: “Error Partitioning: Could not allocate requested partitions: not enough free space on disks.”

10. Verify the USB Drive letter or use the pull-down menu to select a new drive letter.

11. Click OK in the main dialog.
12. A process begins to copy the RHEL image (.iso) file and the MCS installation files to the USB drive.



ISO2USB for CentOS/RedHat

1. Copying ISO Image (Current)

2. Extracting Configuration Files

3. Installing Bootloader

4. Installation Complete

Copying additional files, please wait...

Archive:

Source: C:\MediaCentral_Services_2.2.0_Linux\MediaCentral_Services_2.2_Build_84_Linux.t

Destination: E:\MediaCentral_Services_2.2_Build_84_Linux.tar.gz

Progress: copied 434 of 1677 MB

25%

ISO2USB for CentOS/RedHat

1. Copying ISO Image (Done)

2. Extracting Configuration Files (Done)

3. Installing Bootloader (Done)

4. Installation Complete (Current)

Unplug the USB drive and take it to the machine to be installed.

- Reboot the machine and choose **USB boot** option in the BIOS boot menu.
- Choose **Hard drive** installation method and select **/dev/sdc1** as partition that holds ISO images.
- Use **sda** drive for installation and choose to review the partitioning layout.
- In advanced bootloader options, change drive order to **"sda sdc"**.
- Proceed with the installation.

This process takes 10-20 minutes. Once complete, the USB drive has everything it needs to complete the RHEL and MCS installation.

Copying the RHEL image (.iso) file to the USB drive is a one-time process. To install MCS on more than one server, or to re-install MCS, you do not need to repeat these steps.

13. Click Exit to close the application.

To copy the Gen9 storage controller driver to the USB drive:

1. If you have not already obtained the RAID controller drive, see "Storage Controller Driver for the HP ProLiant Gen9 Server" on page 23 for location and download instructions.
2. With the Installation USB drive still plugged in to the Windows laptop or desktop, copy the RAID controller driver ISO to the root directory on the drive:

   `dd-hpsa-18216-x86_64.iso`

3. Rename the ISO:

   - Old Name: dd-hpsa-18216-x86_64.iso
   - New Name: z_dd-hpsa-18216-x86_64.iso

   Renaming the driver ISO is essential, since the installation script attempts to mount the first ISO it finds as the RHEL ISO. If you do not rename it, the installation will fail.

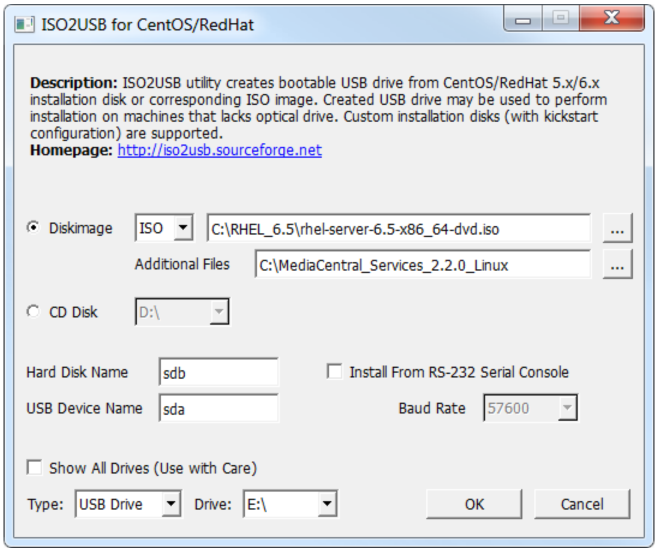
Preparing the Installation Drive for HP Gen8 and Dell Servers

Follow this procedure only if you are installing MCS software components on supported HP Gen8 or Dell servers.

To prepare the MCS Installation USB Drive:

1. Sign into a Windows system.
2. Connect the USB drive to the Windows system and give it a few moments to be recognized.
3. Use Windows Disk Management to format the USB drive as a FAT32 volume.

4. Extract the contents of the MediaCentral_Services_<*version*>_Linux.zip file to the desktop (or your preferred destination directory).
5. Open the newly created MediaCentral_Services_<*version*>_Linux folder.
6. Double-click iso2usb.exe to launch the application.



ISO2USB for CentOS/RedHat

Description: ISO2USB utility creates bootable USB drive from CentOS/RedHat 5.x/6.x installation disk or corresponding ISO image. Created USB drive may be used to perform installation on machines that lacks optical drive. Custom installation disks (with kickstart configuration) are supported.
Homepage: http://iso2usb.sourceforge.net

● Diskimage: ISO — C:\RHEL_6.5\rhel-server-6.5-x86_64-dvd.iso

Additional Files: C:\MediaCentral_Services_2.2.0_Linux

○ CD Disk: D:\

Hard Disk Name: sdb

USB Device Name: sda

□ Install From RS-232 Serial Console

Baud Rate: 57600

□ Show All Drives (Use with Care)

Type: USB Drive

Drive: E:\

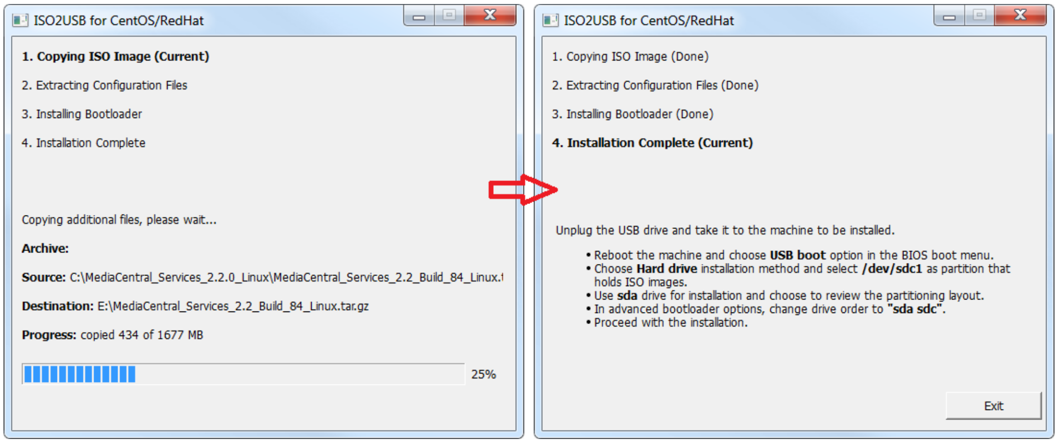
7. Choose the Diskimage radio button then navigate to the RHEL image (.iso) file (named rhel-server-6.5-x86_64-dvd.iso or similar).

Make sure the RHEL image (.iso) file is accessible locally (preferable) or over the network from your computer.

8. In the “Additional Files” field navigate to the MediaCentral_Services_<*version*>_Linux **folder** and click the “Select Folder” button.
9. Verify the Hard Disk Name and USB Device Name fields are as follows:
   - Hard Disk Name: sdb
   - USB Device Name: sda

If the drive names are not configured properly in the kickstart file, you could encounter errors in the deployment process. Example: “Error Partitioning: Could not allocate requested partitions: not enough free space on disks.”

10. Verify the USB Drive letter or use the pull-down menu to select a new drive letter.
11. Click OK in the main dialog.
12. A process begins to copy the RHEL image (.iso) file and the MCS installation files to the USB drive.



ISO2USB for CentOS/RedHat

1. Copying ISO Image (Current)

2. Extracting Configuration Files

3. Installing Bootloader

4. Installation Complete

Copying additional files, please wait...

Archive:

Source: C:\MediaCentral_Services_2.2.0_Linux\MediaCentral_Services_2.2_Build_84_Linux.t

Destination: E:\MediaCentral_Services_2.2_Build_84_Linux.tar.gz

Progress: copied 434 of 1677 MB

25%

ISO2USB for CentOS/RedHat

1. Copying ISO Image (Done)

2. Extracting Configuration Files (Done)

3. Installing Bootloader (Done)

4. Installation Complete (Current)

Unplug the USB drive and take it to the machine to be installed.

- Reboot the machine and choose **USB boot** option in the BIOS boot menu.
- Choose **Hard drive** installation method and select **/dev/sdc1** as partition that holds ISO images.
- Use **sda** drive for installation and choose to review the partitioning layout.
- In advanced bootloader options, change drive order to **"sda sdc"**.
- Proceed with the installation.

This process takes 10-20 minutes. Once complete, the USB drive has everything it needs to complete the RHEL and MCS installation.

Copying the RHEL image (.iso) file to the USB drive is a one-time process. To install MCS on more than one server, or to re-install MCS, you do not need to repeat these steps.

2 BIOS and RAID Configuration

Chapter Overview

The purpose of this chapter is to prepare the server hardware for the installation of RHEL and MCS.

The following table describes the topics covered in this chapter:

Step	Task	Time Est.
1	Changing BIOS Settings	15 min
	Each of the supported server types require adjustments to the system BIOS. This section covers: • HP ProLiant DL360 Gen9 • HP ProLiant DL360p Gen8 • Dell PowerEdge R620 / R630	
2	Configuring the Onboard RAID	*varies*
	Each of the supported server types features different methods for creating and working with the onboard RAID controllers. This section covers: • HP ProLiant DL360 Gen9 • HP ProLiant DL360p Gen8 • Dell PowerEdge R620 / R630	

Changing BIOS Settings

This section provides information on the BIOS settings for the following Avid qualified servers:

- Configuring the BIOS on the HP ProLiant DL360 Gen9
- Configuring the BIOS on the HP ProLiant DL360p Gen8
- Configuring the BIOS on the Dell PowerEdge R620 / R630

Servers are frequently shipped with BIOS settings configured for a power-saving mode. MCS makes intensive use of the server's CPUs and memory, especially when under heavy load. Configuring the server to operate at maximum performance will ensure operational efficiency.

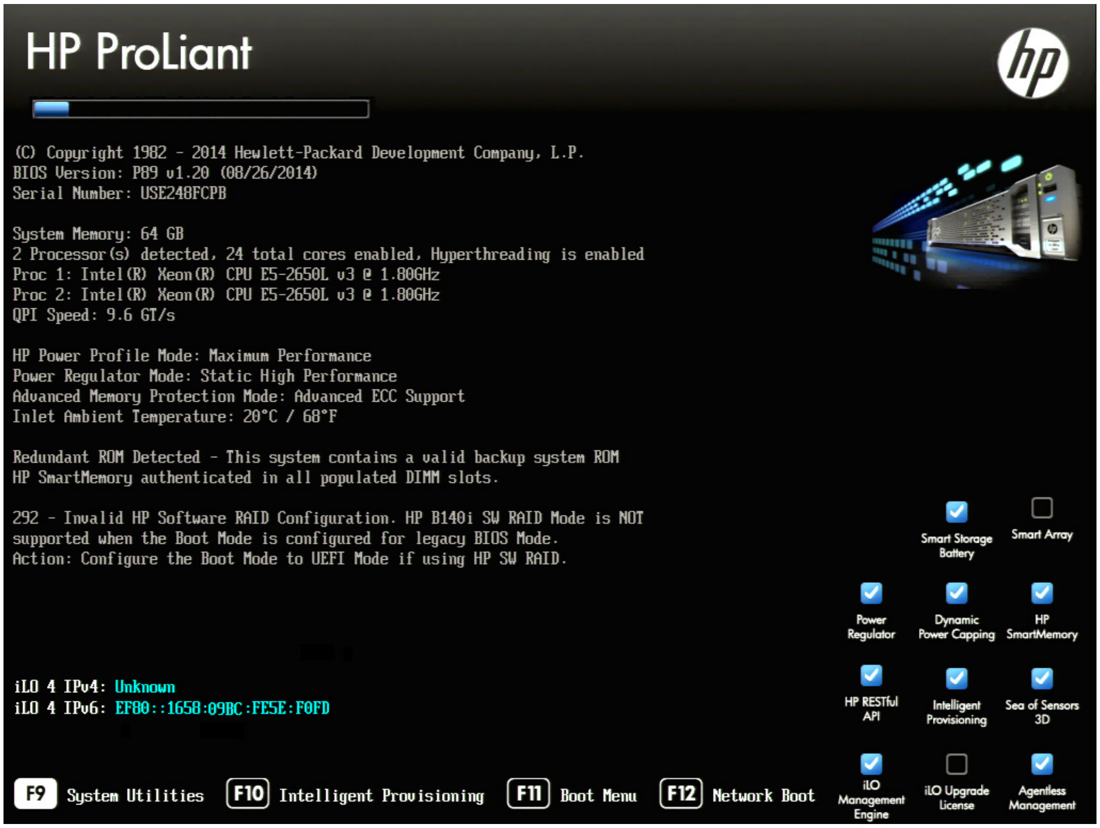
To ensure the smooth installation of RHEL and MCS, the system clock must be set within the BIOS. When configuring an MCS cluster, setting the system clocks accurately is particularly important.

Configuring the BIOS on the HP ProLiant DL360 Gen9

To configure the BIOS on the HP Gen9 server:

1. Power up the server.
2. When the console displays the option to enter the "System Utilities" menu, press F9.

   The BIOS responds by highlighting the F9 icon at the bottom of the screen as depicted below:



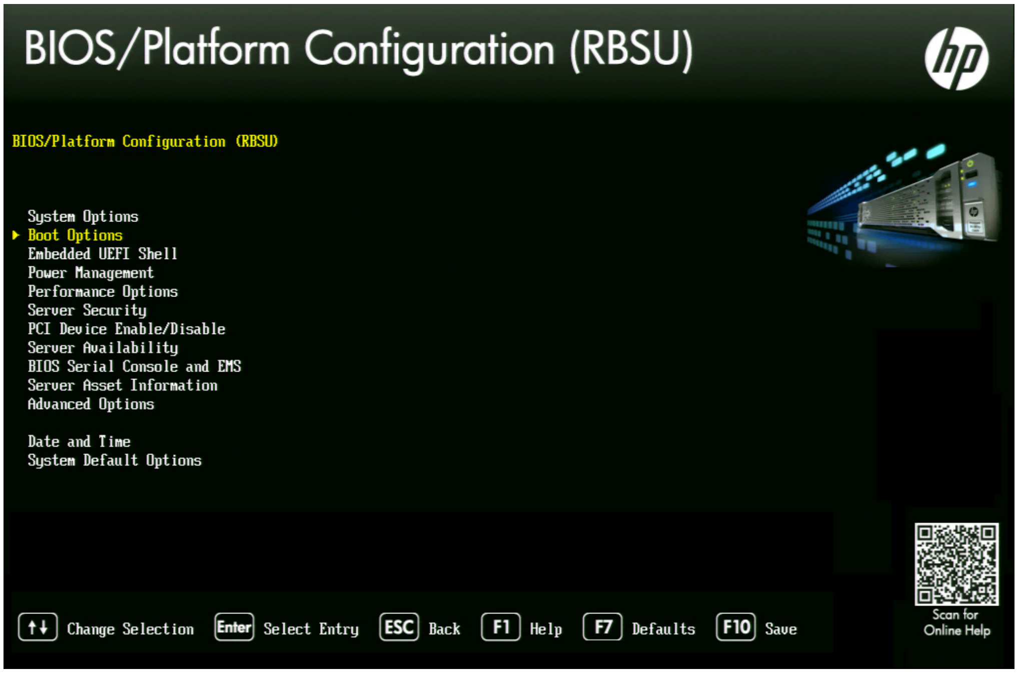
HP ProLiant

```
(C) Copyright 1982 - 2014 Hewlett-Packard Development Company, L.P.
BIOS Version: P89 v1.20 (08/26/2014)
Serial Number: USE248FCPB

System Memory: 64 GB
2 Processor(s) detected, 24 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) CPU E5-2650L v3 @ 1.80GHz
Proc 2: Intel(R) Xeon(R) CPU E5-2650L v3 @ 1.80GHz
QPI Speed: 9.6 GT/s

HP Power Profile Mode: Maximum Performance
Power Regulator Mode: Static High Performance
Advanced Memory Protection Mode: Advanced ECC Support
Inlet Ambient Temperature: 20°C / 68°F

Redundant ROM Detected - This system contains a valid backup system ROM
HP SmartMemory authenticated in all populated DIMM slots.

292 - Invalid HP Software RAID Configuration. HP B140i SW RAID Mode is NOT
supported when the Boot Mode is configured for legacy BIOS Mode.
Action: Configure the Boot Mode to UEFI Mode if using HP SW RAID.



iLO 4 IPv4: Unknown
iLO 4 IPv6: EF80::1658:09BC:FE5E:F0FD
```

☑ Smart Storage Battery
□ Smart Array
☑ Power Regulator
☑ Dynamic Power Capping
☑ HP SmartMemory
☑ HP RESTful API
☑ Intelligent Provisioning
☑ Sea of Sensors 3D
☑ iLO Management Engine
□ iLO Upgrade License
☑ Agentless Management

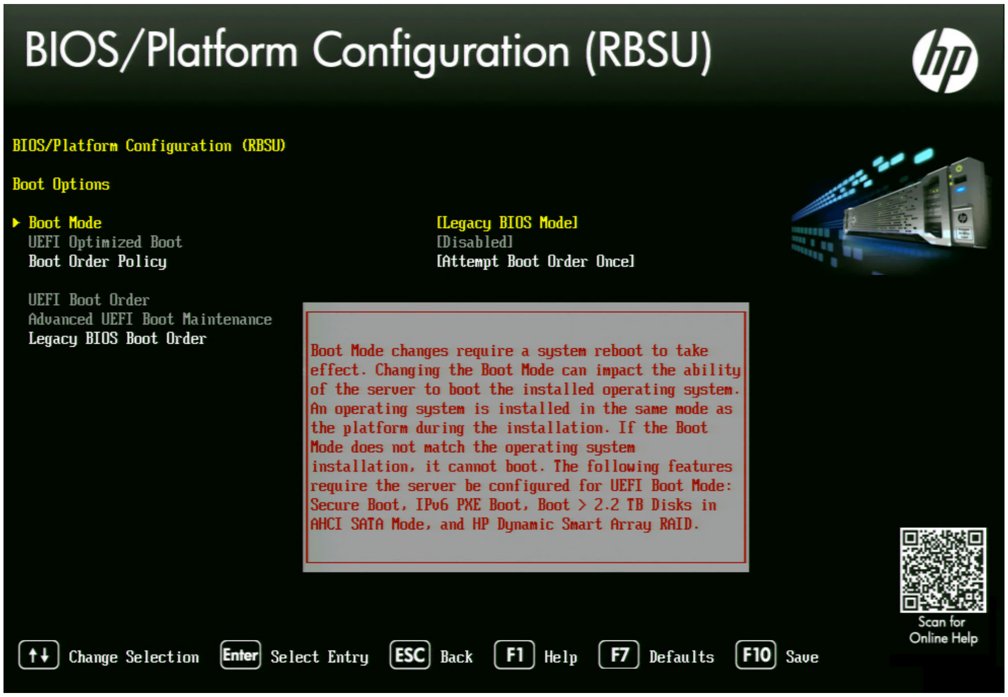
3. Select the **System Configuration** menu item and press Enter.

4. Select the **BIOS/Platform Configuration (RBSU)** menu item and press Enter.



5. Select the **Boot Options** menu item and press Enter.
6. Select the **Boot Mode** menu item and press Enter.

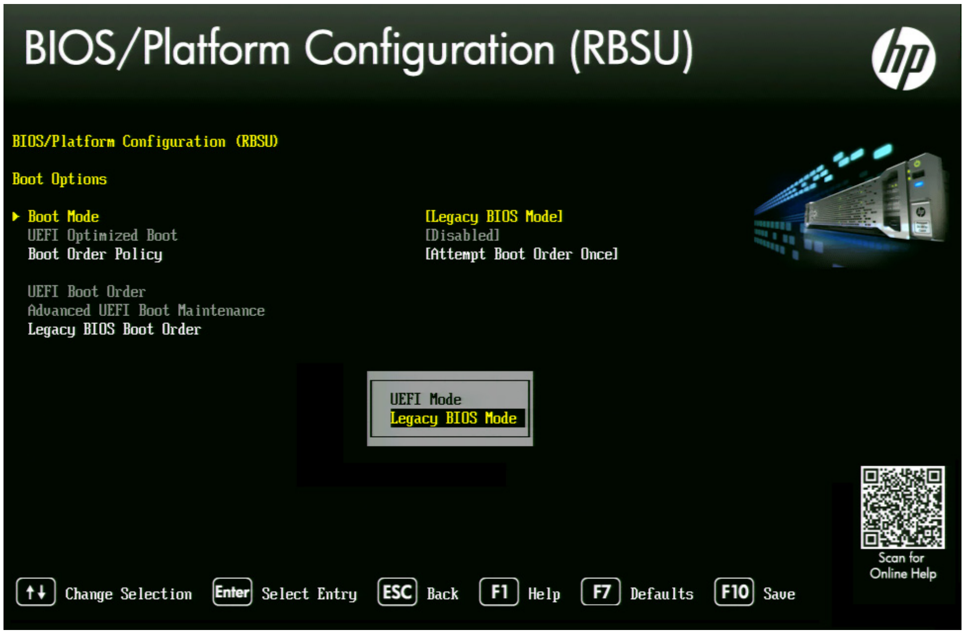
   You may see a warning message (shown below) indicating that Boot Mode changes will require a reboot. Press Enter to acknowledge this message.



```
▸ Boot Mode                    [Legacy BIOS Mode]
  UEFI Optimized Boot          [Disabled]
  Boot Order Policy            [Attempt Boot Order Once]
```

Boot Mode changes require a system reboot to take effect. Changing the Boot Mode can impact the ability of the server to boot the installed operating system. An operating system is installed in the same mode as the platform during the installation. If the Boot Mode does not match the operating system installation, it cannot boot. The following features require the server be configured for UEFI Boot Mode: Secure Boot, IPv6 PXE Boot, Boot > 2.2 TB Disks in AHCI SATA Mode, and HP Dynamic Smart Array RAID.

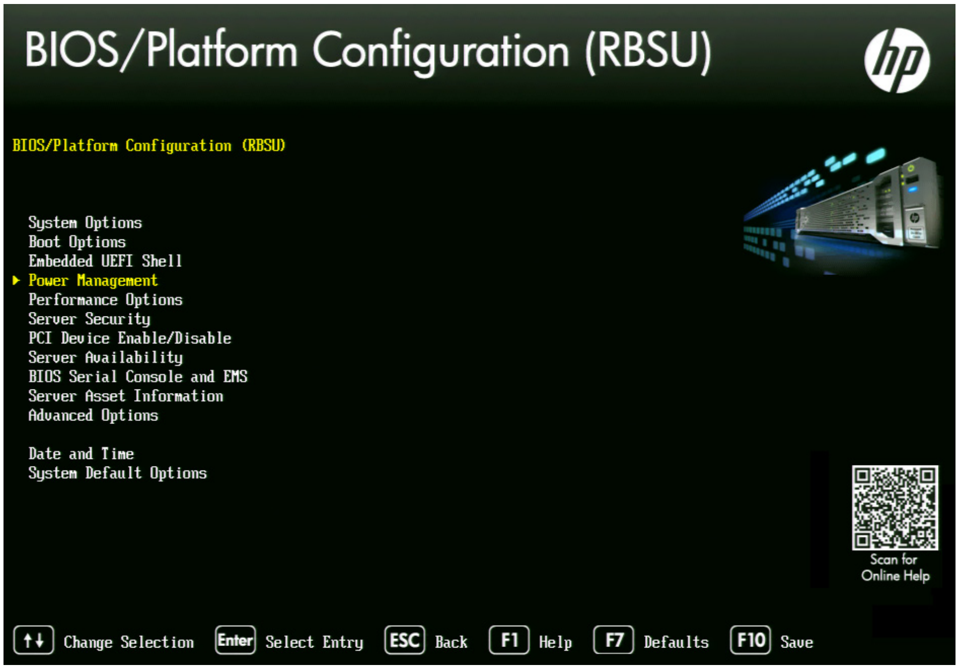
7. A smaller selection box will appear. Select the **Legacy BIOS Mode** menu item and press Enter.



```
BIOS/Platform Configuration (RBSU)

BIOS/Platform Configuration (RBSU)

Boot Options

▸ Boot Mode                                        [Legacy BIOS Mode]
  UEFI Optimized Boot                              [Disabled]
  Boot Order Policy                                [Attempt Boot Order Once]

  UEFI Boot Order
  Advanced UEFI Boot Maintenance
  Legacy BIOS Boot Order

                              UEFI Mode
                              Legacy BIOS Mode
```

8. Press ESC to navigate back to the **BIOS/Platform Configuration (RBSU)** screen.

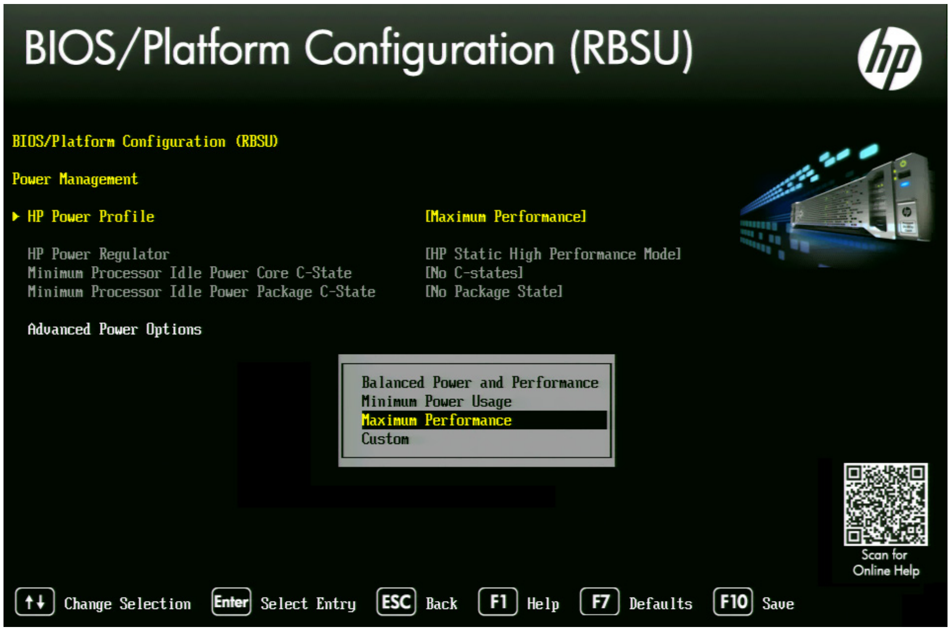
9. Select the **Power Management** menu item and press Enter.



```
BIOS/Platform Configuration (RBSU)

BIOS/Platform Configuration (RBSU)


  System Options
  Boot Options
  Embedded UEFI Shell
▸ Power Management
  Performance Options
  Server Security
  PCI Device Enable/Disable
  Server Availability
  BIOS Serial Console and EMS
  Server Asset Information
  Advanced Options

  Date and Time
  System Default Options
```

10. Press Enter to select **HP Power Profile**.

11. A smaller selection box will appear. Select **Maximum Performance** and press Enter.



BIOS/Platform Configuration (RBSU)

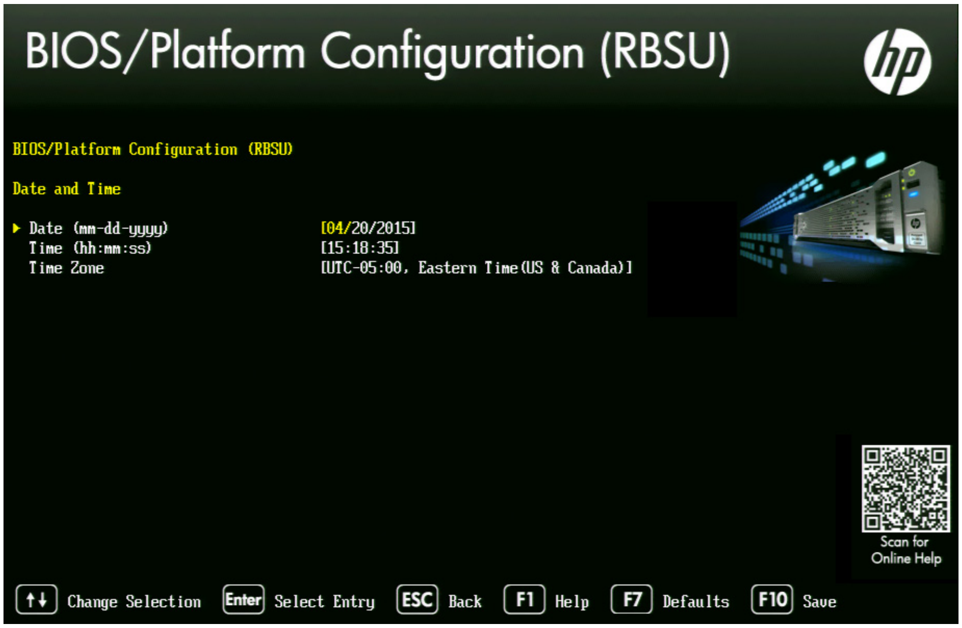
BIOS/Platform Configuration (RBSU)

Power Management

```
▸ HP Power Profile                                  [Maximum Performance]

  HP Power Regulator                                [HP Static High Performance Mode]
  Minimum Processor Idle Power Core C-State         [No C-states]
  Minimum Processor Idle Power Package C-State      [No Package State]

  Advanced Power Options
```

12. Press ESC to navigate back to the **BIOS/Platform Configuration (RBSU)** screen.

13. Select the **Date and Time** menu item and press Enter.



BIOS/Platform Configuration (RBSU)

BIOS/Platform Configuration (RBSU)

Date and Time

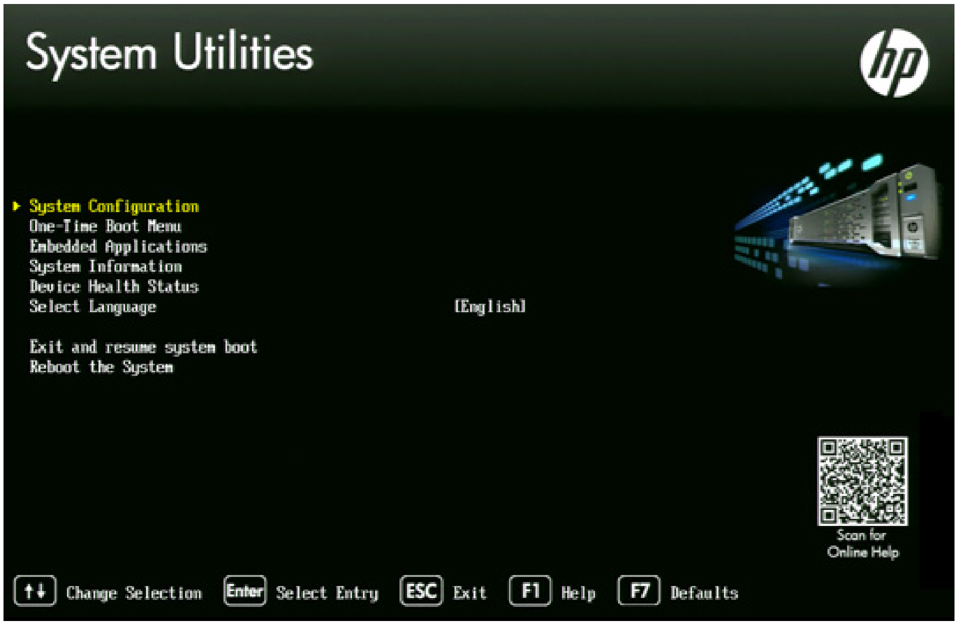
```
▸ Date (mm-dd-yyyy)              [04/20/2015]
  Time (hh:mm:ss)                [15:18:35]
  Time Zone                      [UTC-05:00, Eastern Time(US & Canada)]
```

14. Set the date (mm-dd-yyyy) and time (hh:mm:ss).

15. Press ESC to navigate back to the **BIOS/Platform Configuration (RBSU)** screen.

16. Depending on the options selected at time of purchase, Gen9 HP can be equipped with a 1 GB flash memory partition embedded on the motherboard. During the kickstart assisted USB installation, this partition presents itself as an additional internal HD which causes the process to fail. Disable the Embedded User Partition to avoid problems during the installation.
    a. Select System Options from the **BIOS/Platform Configuration (RBSU)** screen.
    b. Select the **USB Options** menu item and press Enter.
    c. Select the **Embedded User Partition** menu item and press Enter.
    d. Verify that the option is configured for **Disabled** (default).
17. Press **F10** to save.
18. Press ESC to navigate back to the **System Configuration** screen.

    If prompted, select “Y” to save changes and exit.
19. Press ESC to navigate back to the **System Utilities** screen.



Select Language [English]

20. Select **Reboot the System** and press Enter.

    The server reboots with new options.

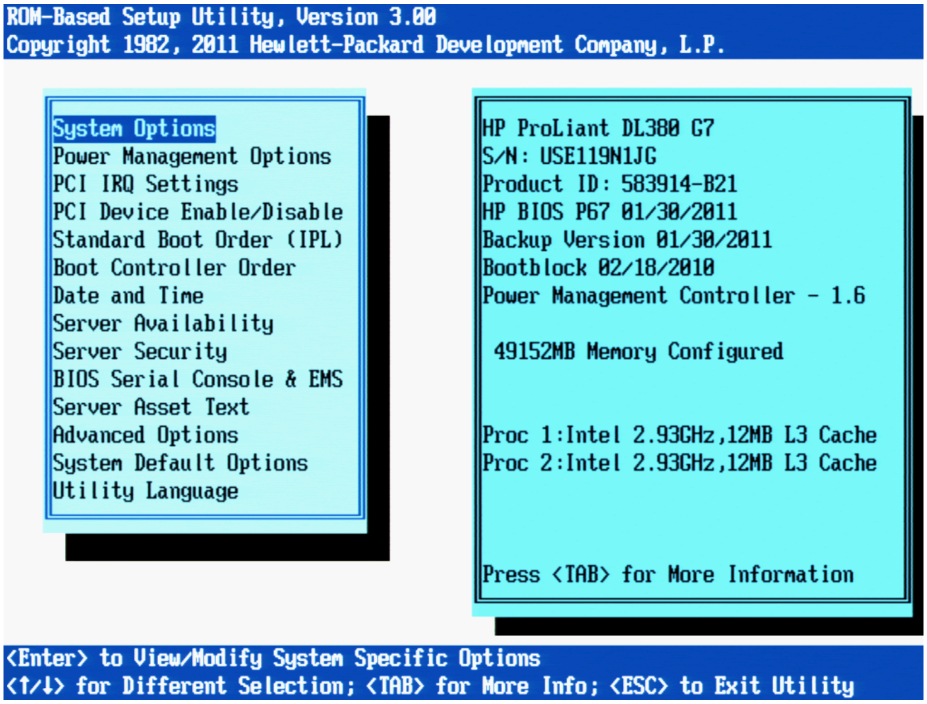
Proceed to “Configuring the Onboard RAID” on page 47.

Configuring the BIOS on the HP ProLiant DL360p Gen8

To configure the BIOS on the HP Gen8 server:

1. Power up the server.
2. When the console displays the option to enter the “System Utilities” menu, press **F9.** The BIOS responds by highlighting the F9 button at the bottom of the screen.

    The ROM-Based Setup Utility appears after a few moments.



```
ROM-Based Setup Utility, Version 3.00
Copyright 1982, 2011 Hewlett-Packard Development Company, L.P.

System Options                     HP ProLiant DL380 G7
Power Management Options           S/N: USE119N1JG
PCI IRQ Settings                   Product ID: 583914-B21
PCI Device Enable/Disable          HP BIOS P67 01/30/2011
Standard Boot Order (IPL)          Backup Version 01/30/2011
Boot Controller Order              Bootblock 02/18/2010
Date and Time                      Power Management Controller - 1.6
Server Availability
Server Security                     49152MB Memory Configured
BIOS Serial Console & EMS
Server Asset Text
Advanced Options                   Proc 1:Intel 2.93GHz,12MB L3 Cache
System Default Options             Proc 2:Intel 2.93GHz,12MB L3 Cache
Utility Language


                                   Press <TAB> for More Information

<Enter> to View/Modify System Specific Options
<↑/↓> for Different Selection; <TAB> for More Info; <ESC> to Exit Utility
```

3. Select **Power Management Options** and press Enter.

   Power Management options are displayed.

4. Choose **HP Power Profile**.

   Power Profile options are displayed.

5. Choose **Maximum Performance**.

   You are returned to the Power Management options menu.

6. Press Esc to return to main menu.
7. Select **Date and Time** and press Enter.

   Date and Time options are displayed.

8. Set the date (mm-dd-yyyy) and time (hh:mm:ss).
9. Press Enter to save the changes and return to the Setup Utility menu.
10. Exit the Setup utility. Press Esc and F10 to save.

    The server reboots with new options.

Proceed to “Configuring the Onboard RAID” on page 47.

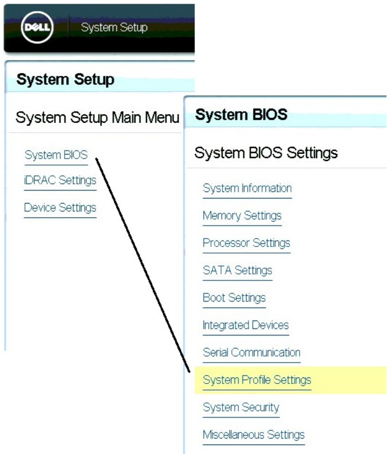
Configuring the BIOS on the Dell PowerEdge R620 / R630

This process includes steps to ensure your MCS Installation USB drive is first in the boot order. Prior to beginning this process, ensure your MCS Installation drive is available.

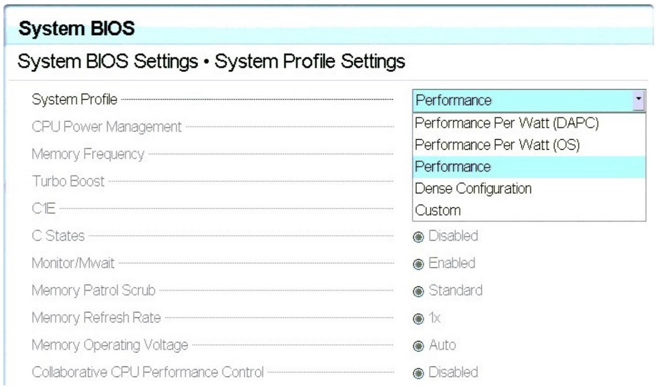
For instructions on creating the boot drive, see “Preparing the Installation Drive for HP Gen8 and Dell Servers” on page 35.

To configure the BIOS on the Dell PowerEdge server:

1. Connect your MCS Installation USB drive to one of the Dell’s USB ports.
2. Power up the server.
3. Press F2 to enter the BIOS.
4. Select **System BIOS**.
5. Select **System Profile Settings**.



6. Select the **Performance** profile from the pull-down menu and click Back.


System BIOS

System BIOS Settings • System Profile Settings

System Profile .... Performance

CPU Power Management ....

Memory Frequency ....

Turbo Boost ....

C1E ....

C States .... ● Disabled

Monitor/Mwait .... ● Enabled

Memory Patrol Scrub .... ● Standard

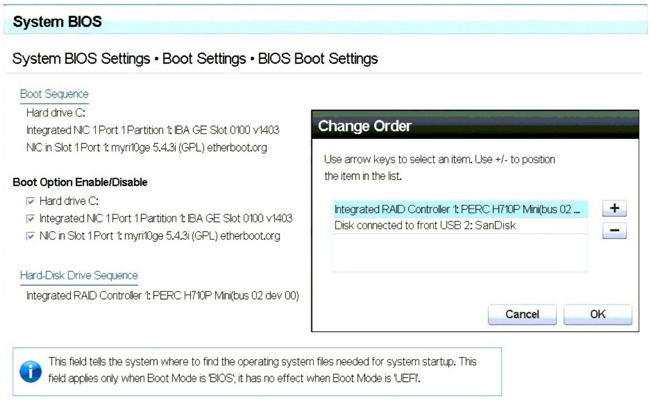
Memory Refresh Rate .... ● 1x

Memory Operating Voltage .... ● Auto

Collaborative CPU Performance Control .... ● Disabled

There are three “Performance” profiles. Once of them specifically says “Performance” and not “Performance Per Watt.”

7. Select **System BIOS Settings**.
8. Select **Boot Settings**.
9. Select **BIOS Boot Settings**.
10. Select **Hard-Disk Drive Sequence**.
11. In the Change Order window, use the + or – keys to move the USB boot drive to the top of the list and click OK.



System BIOS

System BIOS Settings • Boot Settings • BIOS Boot Settings

Boot Sequence
Hard drive C:
Integrated NIC 1 Port 1 Partition 1: IBA GE Slot 0100 v1403
NIC in Slot 1 Port 1: myri10ge 5.4.3i (GPL) etherboot.org

Boot Option Enable/Disable
☑ Hard drive C:
☑ Integrated NIC 1 Port 1 Partition 1: IBA GE Slot 0100 v1403
☑ NIC in Slot 1 Port 1: myri10ge 5.4.3i (GPL) etherboot.org

Hard-Disk Drive Sequence
Integrated RAID Controller 1: PERC H710P Mini(bus 02 dev 00)

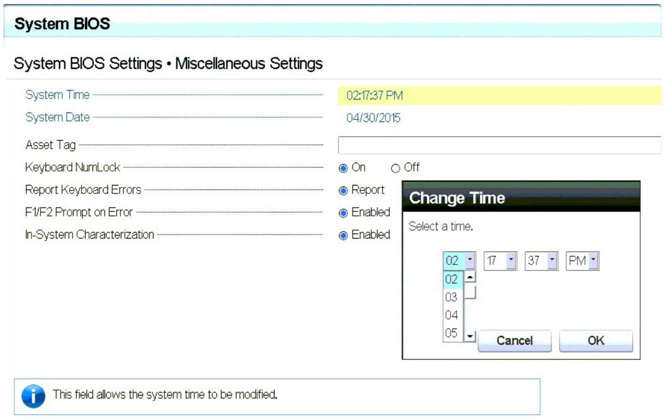
Change Order

Use arrow keys to select an item. Use +/- to position the item in the list.

Integrated RAID Controller 1: PERC H710P Mini(bus 02 ...
Disk connected to front USB 2: SanDisk

This field tells the system where to find the operating system files needed for system startup. This field applies only when Boot Mode is 'BIOS'; it has no effect when Boot Mode is 'UEFI'.

12. Click Back to exit the page and to exit the **System BIOS Settings** page.
13. Select **Miscellaneous Settings**.



System BIOS

System BIOS Settings • Miscellaneous Settings

System Time	02:17:37 PM
System Date	04/30/2015
Asset Tag	
Keyboard NumLock	● On ○ Off
Report Keyboard Errors	● Report
F1/F2 Prompt on Error	● Enabled
In-System Characterization	● Enabled

Change Time

Select a time.

This field allows the system time to be modified.

14. Change the **System Time** and **System Date** by highlighting the appropriate field and pressing Enter.
15. A window will appear with pull-down menu options. Click OK when done.
16. You are asked to confirm the changes.

    A “Success” dialog indicates the settings were saved.
17. Click Back and Finish to return to the main **System Setup** screen.

When ordering a Dell server, an ”Internal SD Card Port” is an optional component. This device will appear to Linux as a media device and it will automatically be assigned a device name. This can interfere with the RHEL / MCS deployment. If you have an “Internal SD Card Port”, temporarily disable it in the BIOS: System BIOS > Integrated Devices > Internal SD Card Port > Off. The device can be re-enabled once you have completed the MCS installation.

Proceed to “Configuring the Onboard RAID” on page 47.

Configuring the Onboard RAID

This section provides information on the RAID configuration for the following Avid qualified servers:

- HP ProLiant DL360 Gen9 RAID Configuration
- HP ProLiant DL360p Gen8 RAID Configuration
- Dell PowerEdge R620 / R630 RAID Configuration

RAID 1: All MCS implementations require a RAID 1 (mirror) for the system (OS) drive. This RAID provides redundancy in the event of HD failure.

RAID 5: Certain deployments also require additional disks configured as a RAID 5 (data striping with parity blocks) for caching file data. This RAID provides redundancy and increased performance.

For more information on RAID configurations, see the *MediaCentral Platform Services Concepts and Clustering Guide*.

HP ProLiant DL360 Gen9 RAID Configuration

In this step you configure two of the HD drives in the server enclosure as a RAID Level 1 – a mirrored RAID – where the RHEL and MCS software will be installed. This is done using the Option ROM Configuration for Arrays utility, in the HP server's BIOS.

If applicable, configure the remaining HD drives in the server enclosure as a RAID Level 5. In a RAID 5 data is automatically distributed across all the disks in the RAID for increased performance and redundancy. This is done using the Option ROM Configuration for Arrays utility, in the HP server's BIOS.

This document provides instructions for creating a media cache volume as a RAID 5 using multiple disks in the server enclosure. However, other configurations are possible, including two drives in a RAID 1 configuration, or a single drive. For details, see the *MediaCentral Platform Services Hardware Guide*.

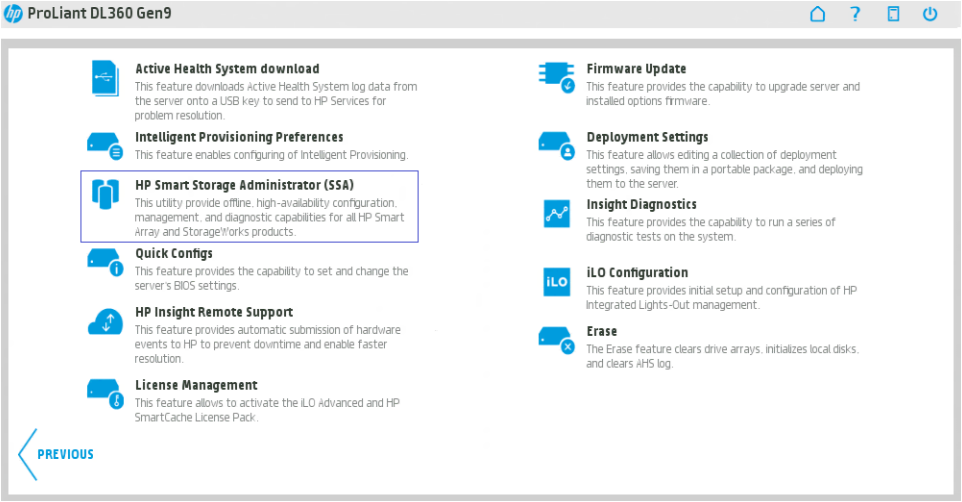
If the list of available disks does not appear as expected, it may be that a RAID has already been created. Deleting a RAID destroys all the data it contains, so verify it is safe to do so first.

The RAID configuration process will immediately transition into the Red Hat / MCS installation. It is recommended that you connect your MCS Installation USB drive to the server at this time.

To configure the HP ProLiant DL360 Gen9 RAID 1:

1. Reboot the server and press **F10** to select **Intelligent Provisioning**.
2. Select **Perform Maintenance**.

3. Select **HP Smart Storage Administrator (SSA)**.



ProLiant DL360 Gen9

Active Health System download
This feature downloads Active Health System log data from the server onto a USB key to send to HP Services for problem resolution.

Intelligent Provisioning Preferences
This feature enables configuring of Intelligent Provisioning.

HP Smart Storage Administrator (SSA)
This utility provide offline, high-availability configuration, management, and diagnostic capabilities for all HP Smart Array and StorageWorks products.

Quick Configs
This feature provides the capability to set and change the server's BIOS settings.

HP Insight Remote Support
This feature provides automatic submission of hardware events to HP to prevent downtime and enable faster resolution.

License Management
This feature allows to activate the iLO Advanced and HP SmartCache License Pack.

Firmware Update
This feature provides the capability to upgrade server and installed options firmware.

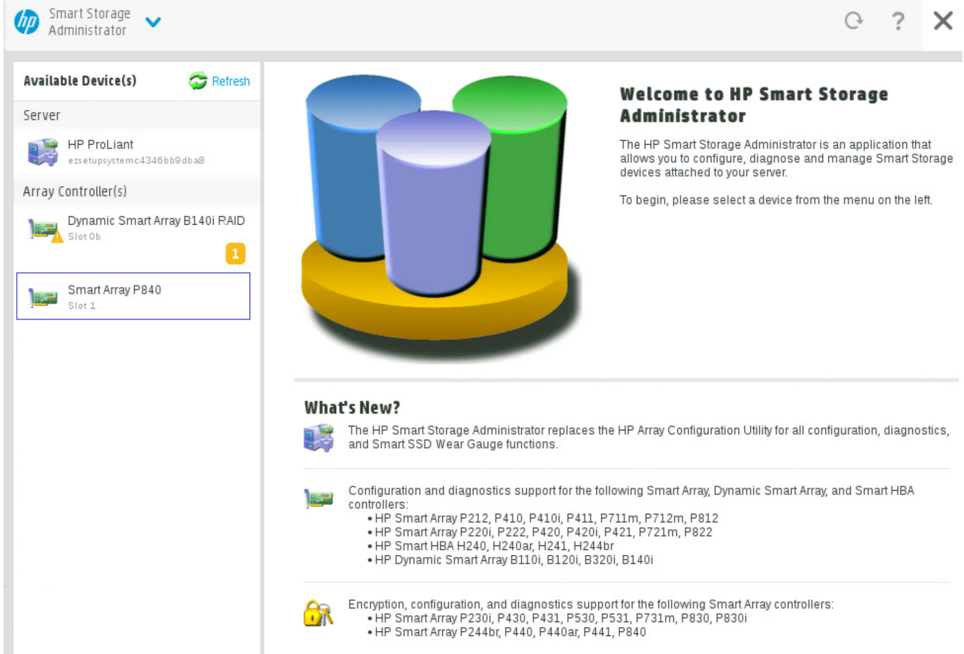
Deployment Settings
This feature allows editing a collection of deployment settings, saving them in a portable package, and deploying them to the server.

Insight Diagnostics
This feature provides the capability to run a series of diagnostic tests on the system.

iLO Configuration
This feature provides initial setup and configuration of HP Integrated Lights-Out management.

Erase
The Erase feature clears drive arrays, initializes local disks, and clears AHS log.

4. At the "Welcome to HP Smart Storage Administrator" screen, select **Smart Array P840** from left side menu.



Welcome to HP Smart Storage Administrator

The HP Smart Storage Administrator is an application that allows you to configure, diagnose and manage Smart Storage devices attached to your server.

To begin, please select a device from the menu on the left.

What's New?

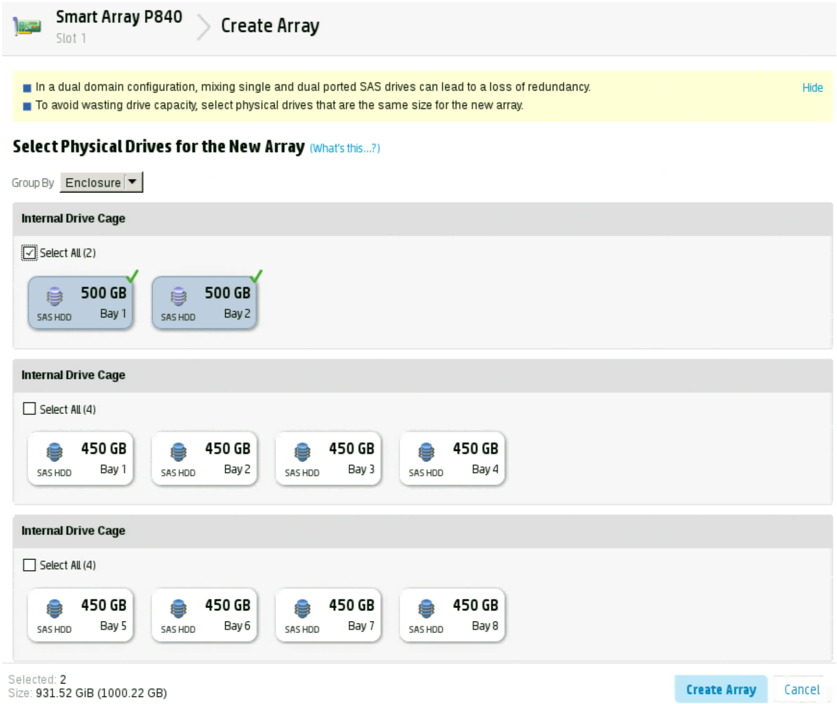
The HP Smart Storage Administrator replaces the HP Array Configuration Utility for all configuration, diagnostics, and Smart SSD Wear Gauge functions.

Configuration and diagnostics support for the following Smart Array, Dynamic Smart Array, and Smart HBA controllers:
- HP Smart Array P212, P410, P410i, P411, P711m, P712m, P812
- HP Smart Array P220i, P222, P420, P420i, P421, P721m, P822
- HP Smart HBA H240, H240ar, H241, H244br
- HP Dynamic Smart Array B110i, B120i, B320i, B140i

Encryption, configuration, and diagnostics support for the following Smart Array controllers:
- HP Smart Array P230i, P430, P431, P530, P531, P731m, P830, P830i
- HP Smart Array P244br, P440, P440ar, P441, P840

5. Select **Create Array** under "Actions".

6. Select both 500GB Drives then select **Create Array**.



Smart Array P840
Slot 1
Create Array

- In a dual domain configuration, mixing single and dual ported SAS drives can lead to a loss of redundancy.
- To avoid wasting drive capacity, select physical drives that are the same size for the new array.

Hide

Select Physical Drives for the New Array (What's this...?)

Group By Enclosure ▼

Internal Drive Cage

☑ Select All (2)

500 GB SAS HDD Bay 1 ✓ | 500 GB SAS HDD Bay 2 ✓

Internal Drive Cage

☐ Select All (4)

450 GB SAS HDD Bay 1 | 450 GB SAS HDD Bay 2 | 450 GB SAS HDD Bay 3 | 450 GB SAS HDD Bay 4

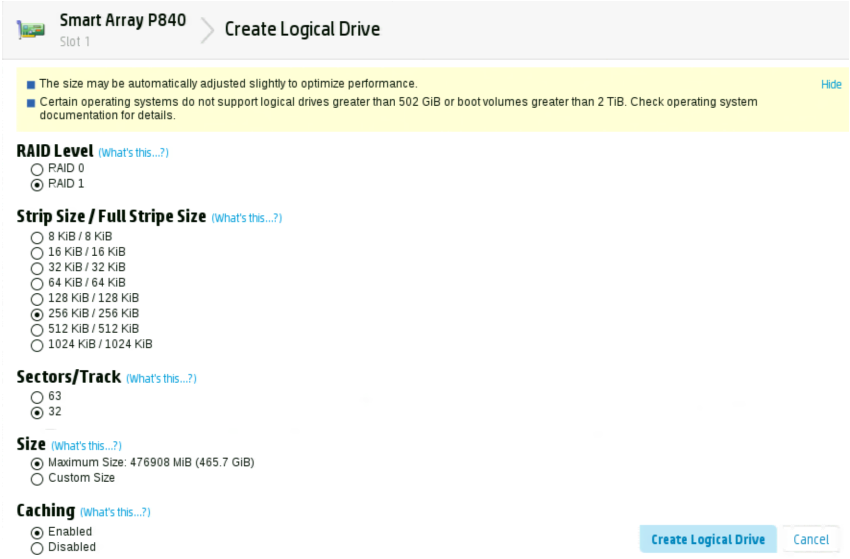
Internal Drive Cage

☐ Select All (4)

450 GB SAS HDD Bay 5 | 450 GB SAS HDD Bay 6 | 450 GB SAS HDD Bay 7 | 450 GB SAS HDD Bay 8

Selected: 2
Size: 931.52 GiB (1000.22 GB)

7. Verify the following are selected: RAID 1, 256 KiB / 256 KiB Stripe Size, 32 Sectors, Maximum Size, Caching Enabled.



Smart Array P840
Slot 1
Create Logical Drive

- The size may be automatically adjusted slightly to optimize performance.
- Certain operating systems do not support logical drives greater than 502 GiB or boot volumes greater than 2 TiB. Check operating system documentation for details.

Hide

RAID Level (What's this...?)
○ RAID 0
● RAID 1

Strip Size / Full Stripe Size (What's this...?)
○ 8 KiB / 8 KiB
○ 16 KiB / 16 KiB
○ 32 KiB / 32 KiB
○ 64 KiB / 64 KiB
○ 128 KiB / 128 KiB
● 256 KiB / 256 KiB
○ 512 KiB / 512 KiB
○ 1024 KiB / 1024 KiB

Sectors/Track (What's this...?)
○ 63
● 32

Size (What's this...?)
● Maximum Size: 476908 MiB (465.7 GiB)
○ Custom Size

Caching (What's this...?)
● Enabled
○ Disabled

8. Click **Create Logical Drive**.

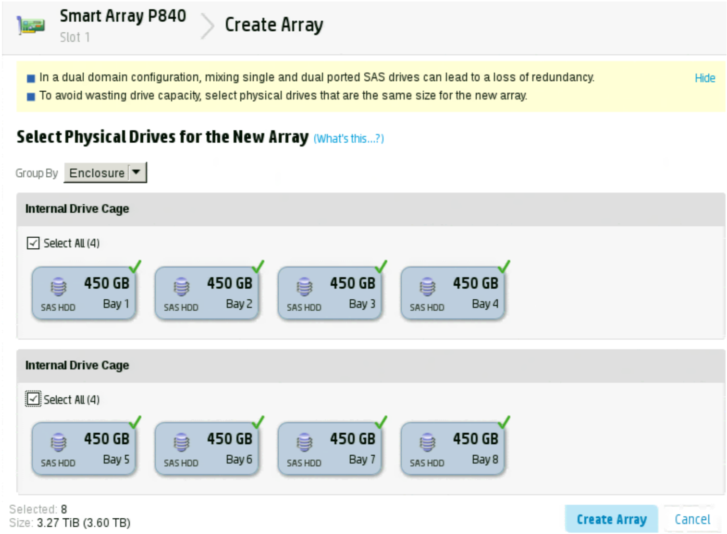
9. You will receive a message indicating the “Logical Drive was successfully created.” Click **Finish** to complete the RAID 1 creation process.

Do not press the Escape key to exit, since this reboots the server.

To configure the HP ProLiant DL360 Gen9 RAID 5:

1. This process assumes you are continuing from the RAID 1 creation process.

   Select **Create Array** under “Actions”.
2. Select all eight 450GB Drives then select **Create Array**.



Smart Array P840
Slot 1
Create Array

- In a dual domain configuration, mixing single and dual ported SAS drives can lead to a loss of redundancy.
- To avoid wasting drive capacity, select physical drives that are the same size for the new array.

Hide

Select Physical Drives for the New Array (What's this...?)

Group By Enclosure ▾

Internal Drive Cage

☑ Select All (4)

450 GB ✓ SAS HDD Bay 1	450 GB ✓ SAS HDD Bay 2	450 GB ✓ SAS HDD Bay 3	450 GB ✓ SAS HDD Bay 4

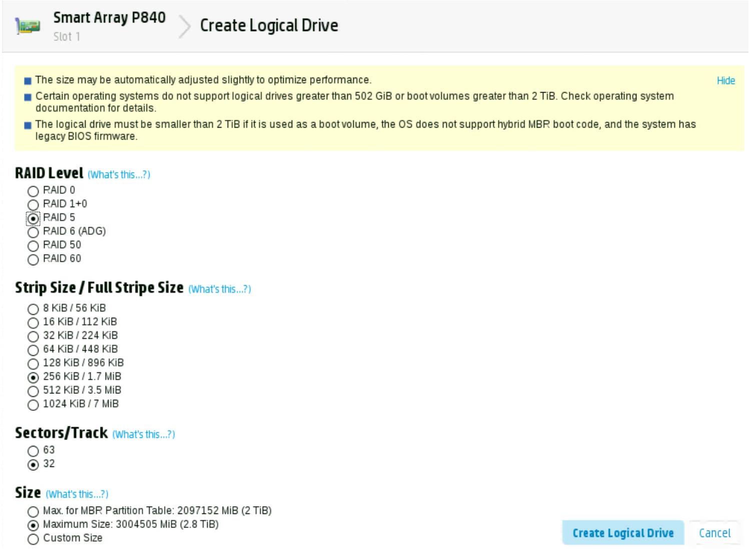
Internal Drive Cage

☑ Select All (4)

450 GB ✓ SAS HDD Bay 5	450 GB ✓ SAS HDD Bay 6	450 GB ✓ SAS HDD Bay 7	450 GB ✓ SAS HDD Bay 8

Selected: 8
Size: 3.27 TiB (3.60 TB)

3. Verify the following are selected: RAID 5, 256 KiB / 1.7 MiB Stripe Size, 32 Sectors, Maximum Size, Caching Enabled.



Smart Array P840
Slot 1
Create Logical Drive

- The size may be automatically adjusted slightly to optimize performance.
- Certain operating systems do not support logical drives greater than 502 GiB or boot volumes greater than 2 TiB. Check operating system documentation for details.
- The logical drive must be smaller than 2 TiB if it is used as a boot volume, the OS does not support hybrid MBR boot code, and the system has legacy BIOS firmware.

Hide

RAID Level (What's this...?)

○ RAID 0
○ RAID 1+0
● RAID 5
○ RAID 6 (ADG)
○ RAID 50
○ RAID 60

Strip Size / Full Stripe Size (What's this...?)

○ 8 KiB / 56 KiB
○ 16 KiB / 112 KiB
○ 32 KiB / 224 KiB
○ 64 KiB / 448 KiB
○ 128 KiB / 896 KiB
● 256 KiB / 1.7 MiB
○ 512 KiB / 3.5 MiB
○ 1024 KiB / 7 MiB

Sectors/Track (What's this...?)

○ 63
● 32

Size (What's this...?)

○ Max. for MBR Partition Table: 2097152 MiB (2 TiB)
● Maximum Size: 3004505 MiB (2.8 TiB)
○ Custom Size

4. Click **Create Logical Drive**.
5. You will receive a message indicating the “Logical Drive was successfully created.” Click **Finish** to complete the RAID 5 creation process.
6. Click the “X” (top right) to exit. Confirm the exit by clicking “OK” when prompted.
7. Click the “Power” button (top right) to exit. Select “Reboot” when prompted.

Proceed to“Software Installation” on page 58 to continue the installation.

HP ProLiant DL360p Gen8 RAID Configuration

In this step you configure two of the HD drives in the server enclosure as a RAID Level 1 – a mirrored RAID – where the RHEL and MCS software will be installed. This is done using the Option ROM Configuration for Arrays utility, in the HP server's BIOS.

If applicable, configure the remaining HD drives in the server enclosure as a RAID Level 5. In a RAID 5, data is automatically distributed across all the disks in the RAID for increased performance and redundancy. This is done using the Option ROM Configuration for Arrays utility, in the HP server's BIOS.

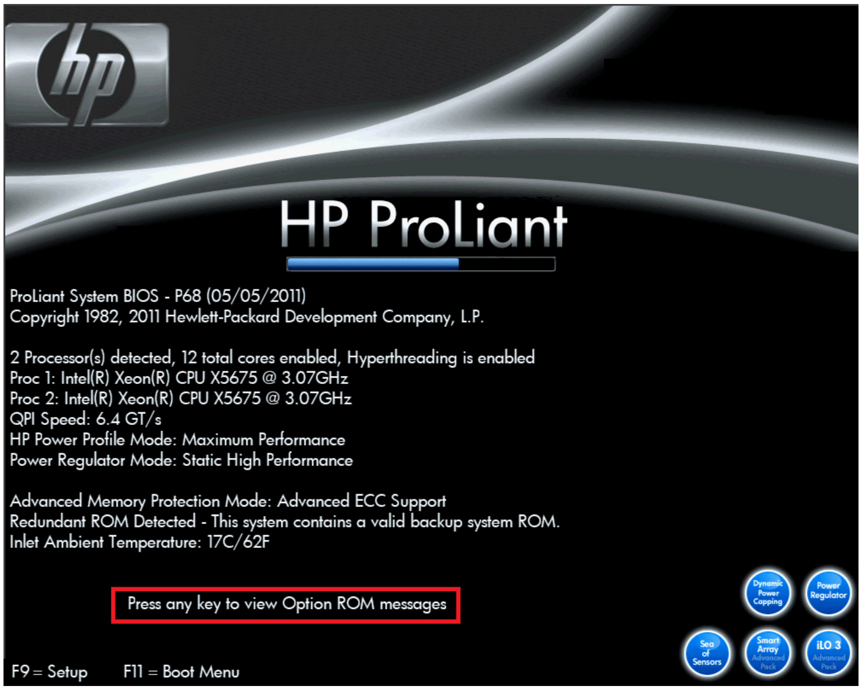
This document provides instructions for creating a media cache volume as a RAID 5 using multiple disks in the server enclosure. However, other configurations are possible, including two drives in a RAID 1 configuration, or a single drive. For details, see the *MediaCentral Platform Services Hardware Guide*.

If the list of available disks does not appear as expected, it may be that a RAID has already been created. Deleting a RAID destroys all the data it contains, so verify it is safe to do so first.

The RAID configuration process will immediately transition into the Red Hat / MCS installation. It is recommended that you connect your MCS Installation USB drive to the server at this time.

To configure the HP ProLiant DL360p Gen8 RAID 1:

1. Reboot the server and press any key (**spacebar** recommended) when prompted to display the HP ProLiant "Option ROM" messages.



ProLiant System BIOS - P68 (05/05/2011)
Copyright 1982, 2011 Hewlett-Packard Development Company, L.P.

2 Processor(s) detected, 12 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) CPU X5675 @ 3.07GHz
Proc 2: Intel(R) Xeon(R) CPU X5675 @ 3.07GHz
QPI Speed: 6.4 GT/s
HP Power Profile Mode: Maximum Performance
Power Regulator Mode: Static High Performance

Advanced Memory Protection Mode: Advanced ECC Support
Redundant ROM Detected - This system contains a valid backup system ROM.
Inlet Ambient Temperature: 17C/62F

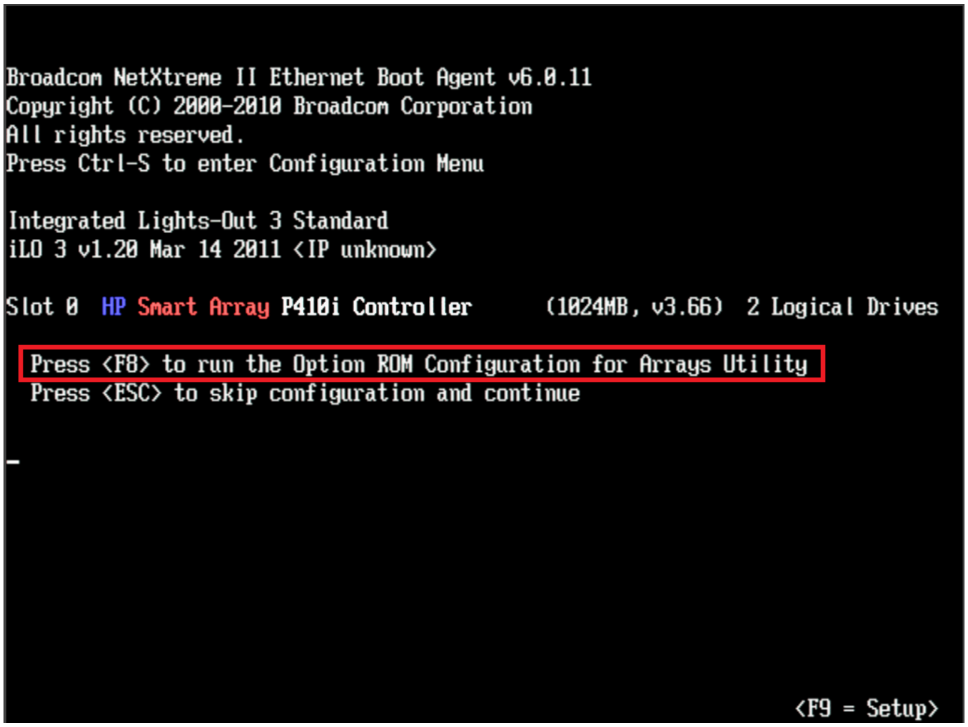
Press any key to view Option ROM messages

F9 = Setup F11 = Boot Menu

Do not press F9 or F11. Press any key other than F9 or F11 (spacebar recommended).

Detailed messages now appear as the server boots up.

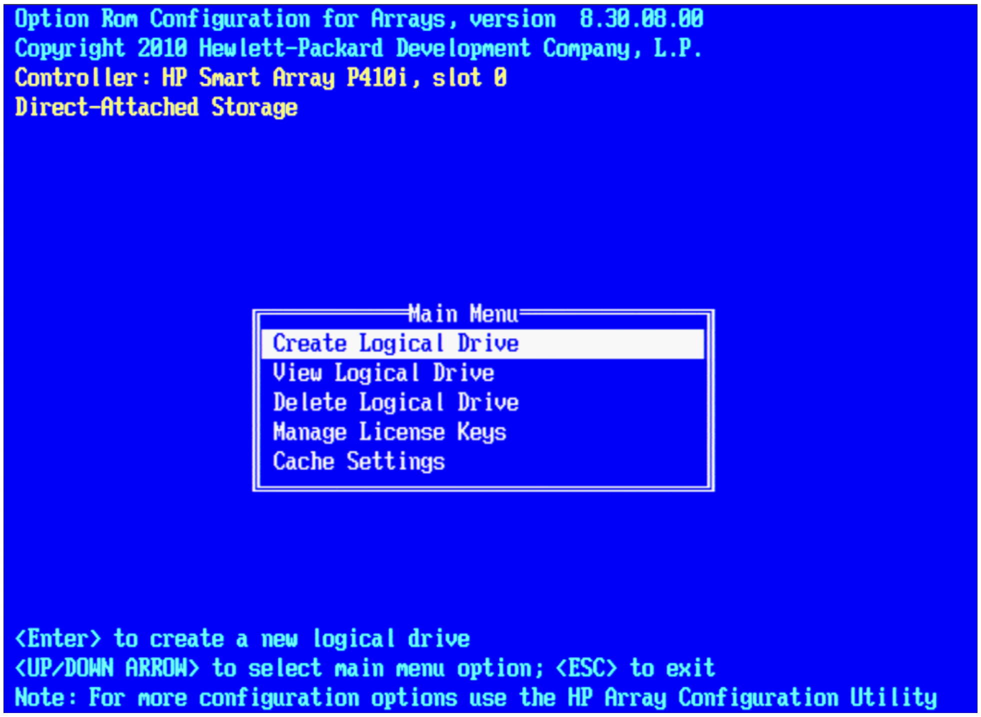
2. As soon as you see the prompt to “Press <F8> to run the Option ROM Configuration for Arrays Utility”, press **F8**.



```
Broadcom NetXtreme II Ethernet Boot Agent v6.0.11
Copyright (C) 2000-2010 Broadcom Corporation
All rights reserved.
Press Ctrl-S to enter Configuration Menu

Integrated Lights-Out 3 Standard
iLO 3 v1.20 Mar 14 2011 <IP unknown>

Slot 0  HP Smart Array P410i Controller      (1024MB, v3.66)  2 Logical Drives

  Press <F8> to run the Option ROM Configuration for Arrays Utility
  Press <ESC> to skip configuration and continue


                                                                <F9 = Setup>
```

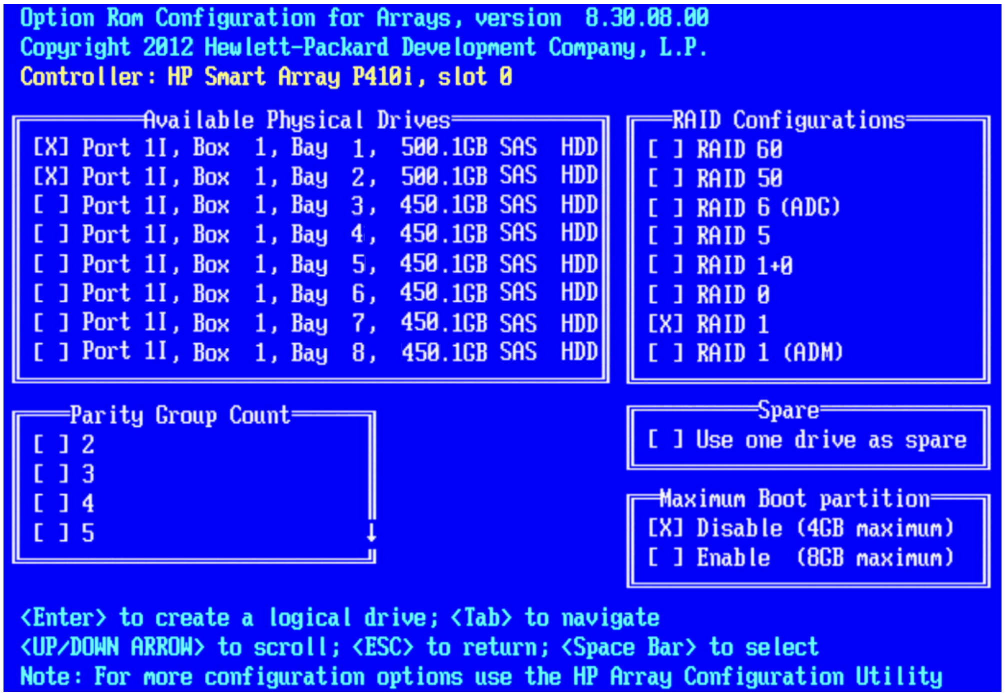
The prompt to press F8 can flash by quite quickly. If you miss it, reboot and try again.

3. From the Main Menu, select **Create Logical Drive**.



```
Option Rom Configuration for Arrays, version  8.30.08.00
Copyright 2010 Hewlett-Packard Development Company, L.P.
Controller: HP Smart Array P410i, slot 0
Direct-Attached Storage

<Enter> to create a new logical drive
<UP/DOWN ARROW> to select main menu option; <ESC> to exit
Note: For more configuration options use the HP Array Configuration Utility
```

4. Select the two HD drives that will serve as the Operating System RAID 1 pair in the “Available Physical Drives” section of the screen. In most cases, these drive are populated in the first two bays (Box 1, Bay 1 and Bay 2).



```
Option Rom Configuration for Arrays, version  8.30.08.00
Copyright 2012 Hewlett-Packard Development Company, L.P.
Controller: HP Smart Array P410i, slot 0

Available Physical Drives                              RAID Configurations
[X] Port 1I, Box  1, Bay  1,  500.1GB SAS  HDD        [ ] RAID 60
[X] Port 1I, Box  1, Bay  2,  500.1GB SAS  HDD        [ ] RAID 50
[ ] Port 1I, Box  1, Bay  3,  450.1GB SAS  HDD        [ ] RAID 6 (ADG)
[ ] Port 1I, Box  1, Bay  4,  450.1GB SAS  HDD        [ ] RAID 5
[ ] Port 1I, Box  1, Bay  5,  450.1GB SAS  HDD        [ ] RAID 1+0
[ ] Port 1I, Box  1, Bay  6,  450.1GB SAS  HDD        [ ] RAID 0
[ ] Port 1I, Box  1, Bay  7,  450.1GB SAS  HDD        [X] RAID 1
[ ] Port 1I, Box  1, Bay  8,  450.1GB SAS  HDD        [ ] RAID 1 (ADM)

Parity Group Count                                     Spare
[ ] 2                                                  [ ] Use one drive as spare
[ ] 3
[ ] 4                                                  Maximum Boot partition
[ ] 5                                                  [X] Disable (4GB maximum)
                                                       [ ] Enable  (8GB maximum)

<Enter> to create a logical drive; <Tab> to navigate
<UP/DOWN ARROW> to scroll; <ESC> to return; <Space Bar> to select
Note: For more configuration options use the HP Array Configuration Utility
```

Notice that the two drives dedicated to the OS in the image above are 500 GB, 7200 RPM whereas the drives that will serve as the RAID 5 are 450 GB, 10K RPM.

5. Deselect all the other available HD drives (if any).
6. Ensure **RAID 1** is selected in the “RAID Configurations” section.

In older firmware versions, the choice presented may be RAID 1+0. Since you are only using two HD drives, this is identical to a RAID 1.

7. Ensure **Disable (4GB maximum)** is selected in the “Maximum Boot partition” section.
8. Ensure nothing is selected in the “Parity Group Count” section.
9. Ensure nothing is selected in the “Spare” section.
10. Press Enter to create the logical drive.

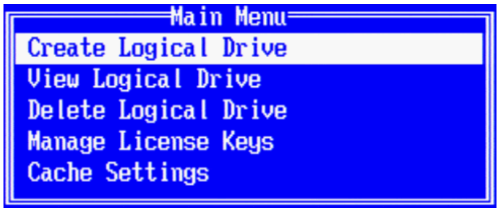
    A message appears summarizing the RAID 1 setup.
11. Press F8 to save the configuration.

    A message appears confirming the configuration has been saved.
12. Press Enter to finalize the RAID 1 setup.

To configure the HP ProLiant DL360p Gen8 RAID 5:

1. This process assumes you are continuing from the RAID 1 creation process.

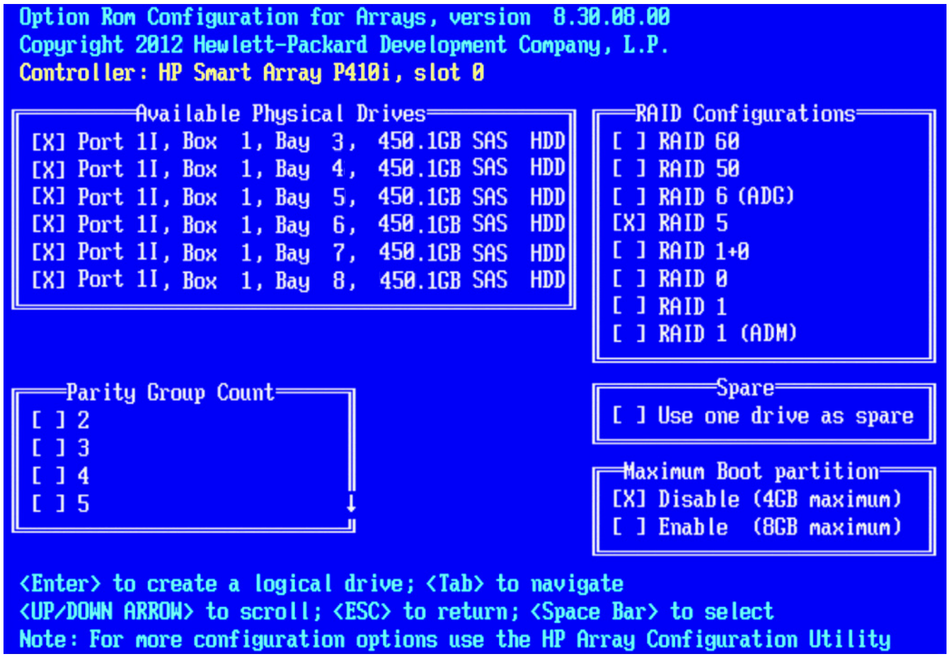
   From the Main Menu, select **Create Logical Drive**.



```
Main Menu
Create Logical Drive
View Logical Drive
Delete Logical Drive
Manage License Keys
Cache Settings
```

2. Select the drives to be included in the RAID 5 in the “Available Physical Drives” section.

   In a typical configuration, Box 1, Bays 3-8 are selected.



```
Option Rom Configuration for Arrays, version  8.30.08.00
Copyright 2012 Hewlett-Packard Development Company, L.P.
Controller: HP Smart Array P410i, slot 0

Available Physical Drives                              RAID Configurations
[X] Port 1I, Box  1, Bay  3,  450.1GB SAS  HDD         [ ] RAID 60
[X] Port 1I, Box  1, Bay  4,  450.1GB SAS  HDD         [ ] RAID 50
[X] Port 1I, Box  1, Bay  5,  450.1GB SAS  HDD         [ ] RAID 6 (ADG)
[X] Port 1I, Box  1, Bay  6,  450.1GB SAS  HDD         [X] RAID 5
[X] Port 1I, Box  1, Bay  7,  450.1GB SAS  HDD         [ ] RAID 1+0
[X] Port 1I, Box  1, Bay  8,  450.1GB SAS  HDD         [ ] RAID 0
                                                       [ ] RAID 1
                                                       [ ] RAID 1 (ADM)

Parity Group Count                                     Spare
[ ] 2                                                  [ ] Use one drive as spare
[ ] 3
[ ] 4                                                  Maximum Boot partition
[ ] 5                                                  [X] Disable (4GB maximum)
                                                       [ ] Enable  (8GB maximum)

<Enter> to create a logical drive; <Tab> to navigate
<UP/DOWN ARROW> to scroll; <ESC> to return; <Space Bar> to select
Note: For more configuration options use the HP Array Configuration Utility
```

3. Ensure **RAID 5** is selected in the “RAID Configurations” section.
4. Ensure **Disable (4GB maximum)** is selected in the “Maximum Boot partition” section.
5. Ensure nothing is selected in the “Parity Group Count” section.
6. Ensure nothing is selected in the “Spare” section.
7. Press Enter to create the logical drive.

   A message appears summarizing the RAID 5 setup.
8. Press F8 to save the configuration.

   A message appears confirming the configuration has been saved.
9. Press Enter to finalize the RAID 5.
10. Press ESC to reboot the system.

Proceed to“Software Installation” on page 58 to continue the installation.

Dell PowerEdge R620 / R630 RAID Configuration

The Dell R620 / R630 servers ship with preconfigured RAID 1 and RAID 5 arrays. In this step you verify the RAID configuration through the BIOS. Later you will use RHEL to ensure the RAID arrays are cleared of existing data.

Two of the HD drives in the server are configured as a RAID Level 1 – a mirrored RAID – where the RHEL and MCS software will be installed.

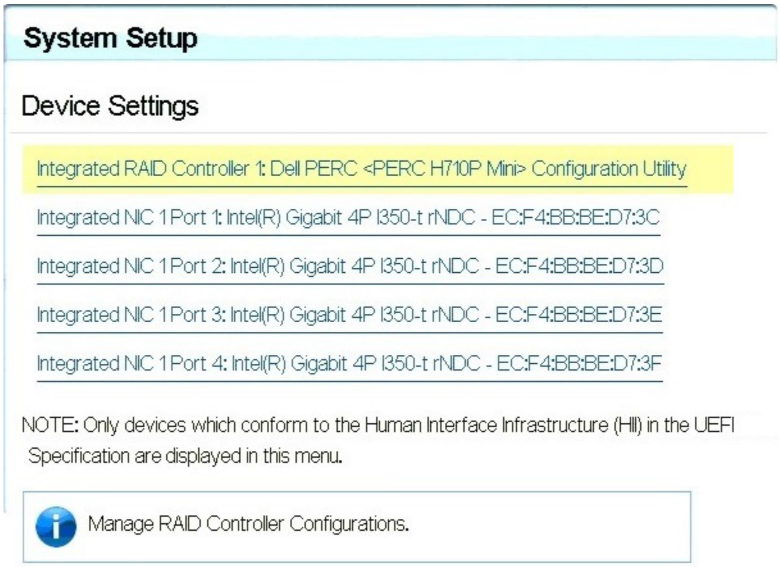
If applicable, the remaining drives in the server enclosure will be configured as a RAID Level 5. In a RAID 5 data is automatically distributed across all the disks in the RAID for increased performance and redundancy.

This document provides instructions for creating a media cache volume as a RAID 5 using multiple disks in the server enclosure. However, other configurations are possible, including two drives in a RAID 1 configuration, or a single drive. For details, see the MediaCentral Platform Services Hardware Guide.

The RAID configuration process will immediately transition into the Red Hat / MCS installation. If you do not already have the MCS Installation USB drive connected, connect it to the server at this time.

To verify the PowerEdge Dell R620 / 630 RAID Configuration:

1. (if necessary) Reboot the server and press F2 to enter the BIOS.
2. From the main **System Setu**p screen, select **Device Settings**.
3. From the **Device Settings** menu, select **Integrated RAID Controller Configuration Utility**.



System Setup

Device Settings

Integrated RAID Controller 1: Dell PERC <PERC H710P Mini> Configuration Utility

Integrated NIC 1 Port 1: Intel(R) Gigabit 4P I350-t rNDC - EC:F4:BB:BE:D7:3C

Integrated NIC 1 Port 2: Intel(R) Gigabit 4P I350-t rNDC - EC:F4:BB:BE:D7:3D

Integrated NIC 1 Port 3: Intel(R) Gigabit 4P I350-t rNDC - EC:F4:BB:BE:D7:3E

Integrated NIC 1 Port 4: Intel(R) Gigabit 4P I350-t rNDC - EC:F4:BB:BE:D7:3F

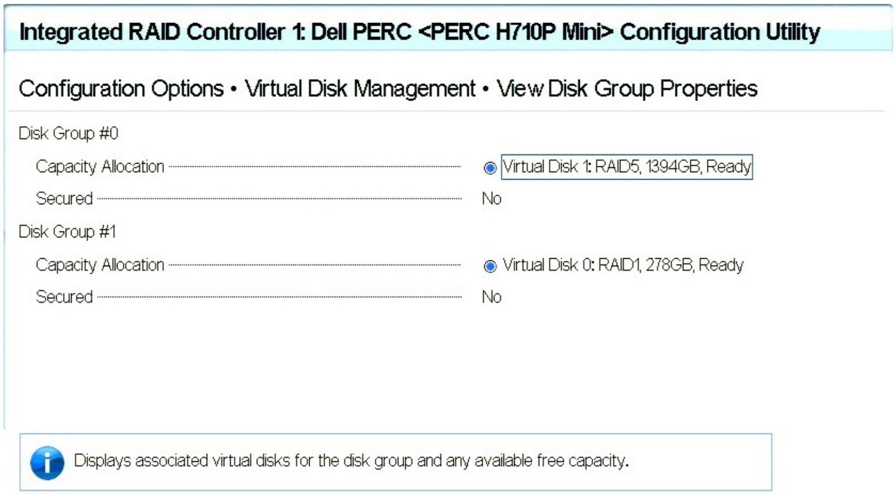
NOTE: Only devices which conform to the Human Interface Infrastructure (HII) in the UEFI Specification are displayed in this menu.

Manage RAID Controller Configurations.

4. From the **Configuration Options** menu, select **Virtual Disk Management**.

5. From the **Virtual Disk Management** menu, select **View Disk Properties**.

   This window lists the configured RAID Groups on the server. You should see both a RAID 1 set and a RAID 5 set.



Integrated RAID Controller 1: Dell PERC <PERC H710P Mini> Configuration Utility

Configuration Options • Virtual Disk Management • View Disk Group Properties

Disk Group #0

Capacity Allocation .... ● Virtual Disk 1: RAID5, 1394GB, Ready

Secured .... No

Disk Group #1

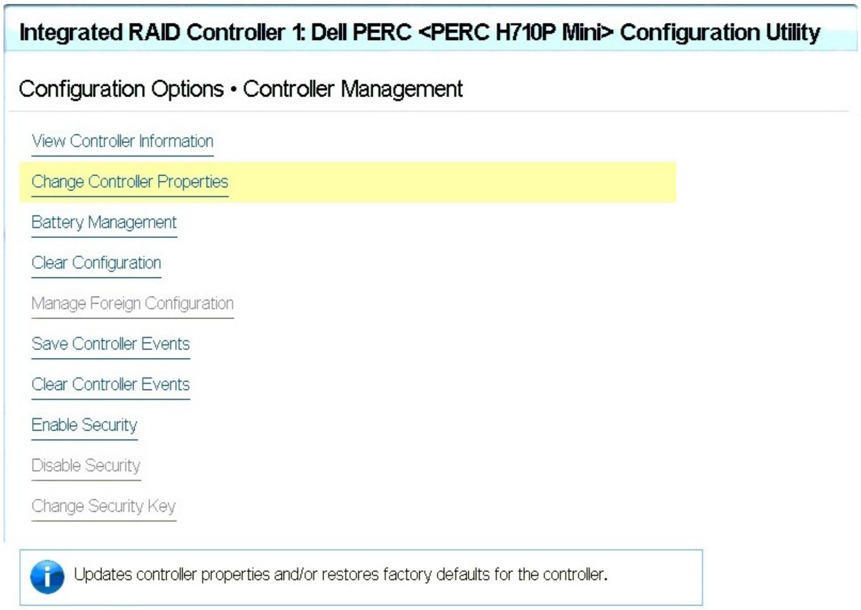
Capacity Allocation .... ● Virtual Disk 0: RAID1, 278GB, Ready

Secured .... No

Displays associated virtual disks for the disk group and any available free capacity.

If the preconfigured RAID arrays do not exist, see “Working with the Dell RAID Controller” on page 243 for information on creating the RAID.

6. From the **Configuration Options** menu, select **Controller Management**.
7. From the **Controller Management** menu, select **Change Controller Properties**.

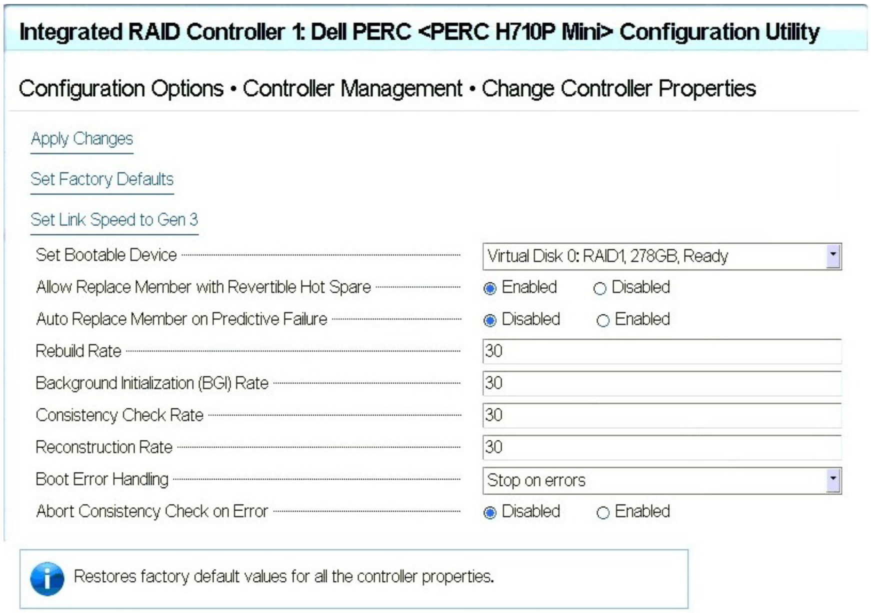


Integrated RAID Controller 1: Dell PERC <PERC H710P Mini> Configuration Utility

Configuration Options • Controller Management

Updates controller properties and/or restores factory defaults for the controller.

8. Ensure the **Set Bootable Device** pull-down menu is configured for **Virtual Disk 0: RAID 1**.



Integrated RAID Controller 1: Dell PERC <PERC H710P Mini> Configuration Utility

Configuration Options • Controller Management • Change Controller Properties

Apply Changes

Set Factory Defaults

Set Link Speed to Gen 3

Set Bootable Device	Virtual Disk 0: RAID1, 278GB, Ready
Allow Replace Member with Revertible Hot Spare	● Enabled ○ Disabled
Auto Replace Member on Predictive Failure	● Disabled ○ Enabled
Rebuild Rate	30
Background Initialization (BGI) Rate	30
Consistency Check Rate	30
Reconstruction Rate	30
Boot Error Handling	Stop on errors
Abort Consistency Check on Error	● Disabled ○ Enabled

Restores factory default values for all the controller properties.

9. Return to the main **System Setup** screen.
10. Click **Finish** to reboot the system.

Proceed to“Software Installation” on page 58 to continue the installation.

3 Software Installation

Chapter Overview

The purpose of this chapter is to assist you with the installation and configuration of the system software.

How to proceed:

- If you are installing MCS on a Dell server, additional steps are required during the server imaging process. Proceed to "Special Instructions for Dell Servers" on page 60 to continue.
- If you are installing MCS on an HP server, proceed directly to "MCS Software Deployment" on page 64.

Both processes use the MCS Installation USB drive to install RedHat and MediaCentral Platform Services. Earlier in this document, you were instructed to create the USB installation drive using specific drive names (sda, sdb, sdc). If your server includes any devices that could identified by RHEL as a volume such as an optical drive or an SD card slot, these devices must be disabled through the system BIOS prior to the software installation. Failure to do so could result in errors during the deployment process, such as: "Error Partitioning: Could not allocate requested partitions: not enough free space on disks."

For details on upgrading from an earlier software release, see the *Avid MediaCentral Platform Services Upgrade Guide* and the *Avid MediaCentral Platform Services ReadMe* available on the Avid Knowledge Base.

The following table describes the topics covered in this chapter:

Step	Task	Time Est.
1	Special Instructions for Dell Servers	10 min
	Covers the deletion of any existing partitions on the Dell RAID arrays prior to the installation of RHEL and MCS.	
2	MCS Software Deployment	30 min
	Covers the actual installation of RHEL and MCS.	
3	Booting RHEL for the First Time	5 min
	Covers keyboard layout configuration and a process for changing the default 'root' user password.	
4	Network Configuration	30 min
	Guides you through the configuration of all network-related settings.	
4	Configuring Access for External Systems	30 min
	A configuration file must be added to allow access of external systems.	

Step	Task	Time Est.
5	Configuring Date and Time Settings	15 min
	Configuration of Date, Time, Time Zone and NTP settings.	
6	Creating the File Cache on the RAID	15 min
	If a RAID 5 array is used, this step finalizes the creation of the RAID 5.	
7	Enabling / Disabling 3G and Edge Streams	2 min
	Instructions for enabling / disabling 3G and Edge streams.	
8	Copying Software to the MCS Server	*varies*
	While RHEL and MCS software is installed by the MCS Installation USB drive, additional software might be required.	
9	Installing Security Updates	15 min
	Information regarding Security Updates for RHEL.	
10	Installing Software Patches	15 min
	A reminder to install available software patches.	
11	Upgrading the Avid Shared Storage Client Software	10 min
	In the event than an updated version of the Avid shared storage client software is required for your environment, client upgrade instructions have been provided.	

Special Instructions for Dell Servers

Dell servers are generally shipped with preconfigured RAID 1 and RAID 5 arrays. These RAID sets include partitions that can interfere with the kickstart assisted software deployment. The partitions must be deleted prior to starting the installation.

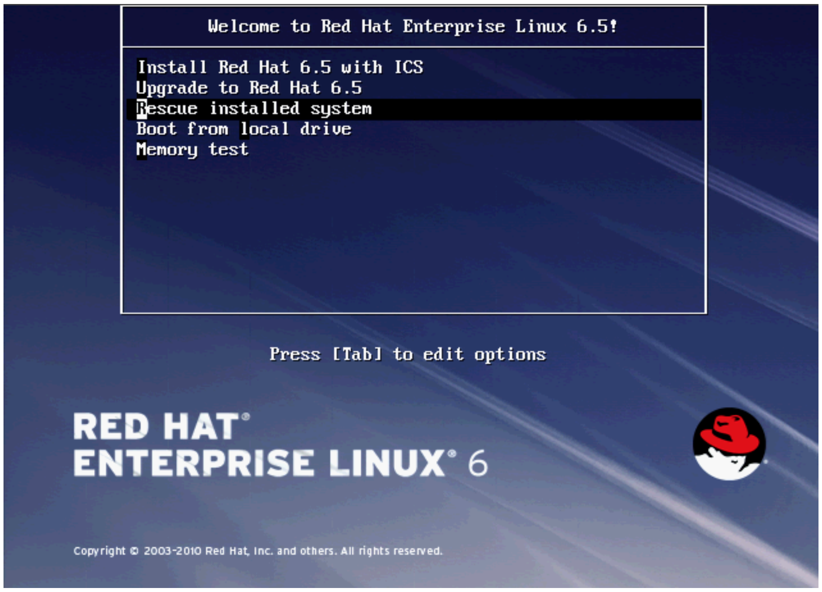
Deleting and recreating the RAID sets using the DELL BIOS utility does not erase data, nor does it delete existing partitions. That is, deleting a RAID does not delete the partition table — unless you initialize the disk at the same time. However, initializing the disk is a slow process.

In this procedure, you boot from the MCS Installation USB Drive and launch a RHEL "rescue" session in order to examine the current system partitions and delete them.

If you are installing MCS on an HP server, proceed to "MCS Software Deployment" on page 64.

To format the disk partitions on the Dell server:

1. Boot from the MCS Installation USB drive.
2. At the RHEL Welcome screen, select "Rescue Installed System".

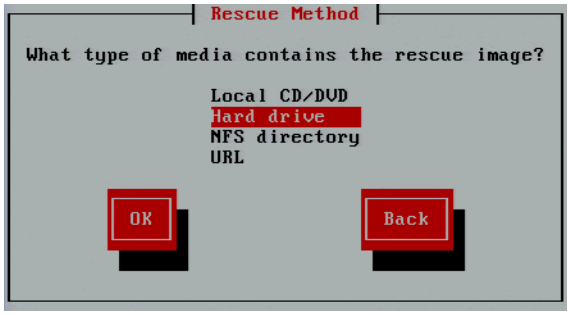


Welcome to Red Hat Enterprise Linux 6.5!

Press [Tab] to edit options

Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

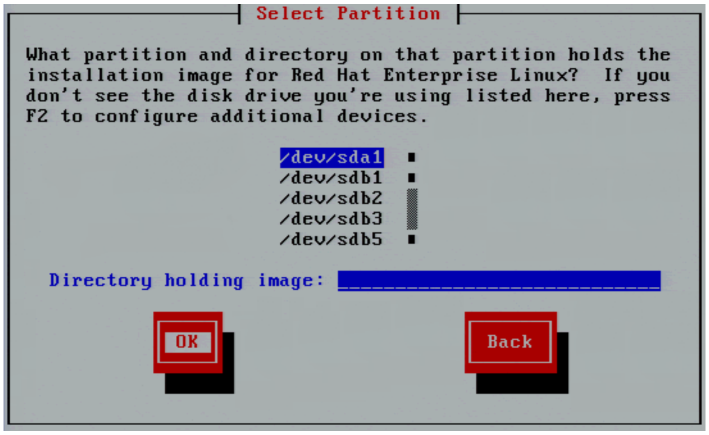
3. When prompted choose the language and keyboard.
4. Choose "Hard drive" as the rescue method. For the purposes of booting from a RHEL image, the USB drive is considered a hard drive.



Rescue Method

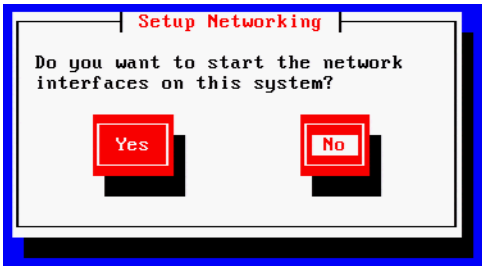
What type of media contains the rescue image?

5. Select the “/dev/sda1” partition (the USB drive). Leave the “Directory holding image” field blank.



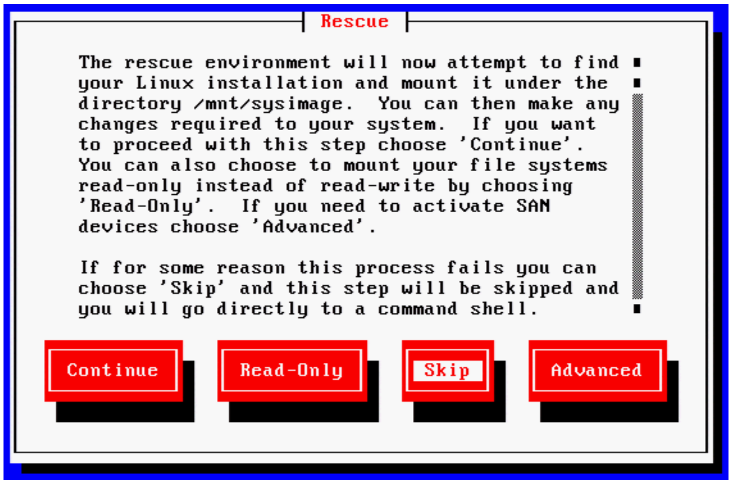
```
What partition and directory on that partition holds the
installation image for Red Hat Enterprise Linux?  If you
don't see the disk drive you're using listed here, press
F2 to configure additional devices.

                    /dev/sda1
                    /dev/sdb1
                    /dev/sdb2
                    /dev/sdb3
                    /dev/sdb5

  Directory holding image:
```

6. Select “No” in the Setup Networking window; as networking is not needed at this time.



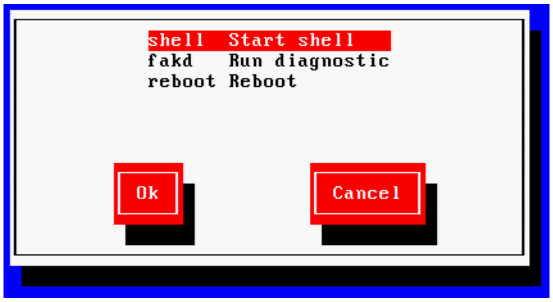
```
Do you want to start the network
interfaces on this system?
```

7. Select “Skip” in the Rescue window.



```
The rescue environment will now attempt to find
your Linux installation and mount it under the
directory /mnt/sysimage.  You can then make any
changes required to your system.  If you want
to proceed with this step choose 'Continue'.
You can also choose to mount your file systems
read-only instead of read-write by choosing
'Read-Only'.  If you need to activate SAN
devices choose 'Advanced'.

 If for some reason this process fails you can
choose 'Skip' and this step will be skipped and
you will go directly to a command shell.
```

8. At the next screen, choose “shell   Start shell” and select Ok.



9. At the system prompt, use the RHEL fdisk utility to examine the current partitions:

   ```
   fdisk -cul
   ```

   This command will display the available disks and partitions on the system. Use Shift-Pg Up and Shift-Pg Down to view the entire output, since scroll bars will not be present in the rescue shell.

   In this case “sda” should be the USB boot drive, “sdb” should be the RAID 1 volume and “sdc” should be the RAID 5 volume.

   The following example shows information for “sdb” with three partitions (sdb1, sdb2, sdb3):

   ```
   Disk /dev/sdb: 500.1 GB, 500074307584 bytes
   255 heads, 63 sectors/track, 60797 cylinders, total 97670732 sectors
   Units = sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disk identifier: 0xc755f5b0

      Device Boot      Start         End      Blocks   Id  System
   /dev/sdb1   *        2048     1026047      512000   83  Linux
   /dev/sdb2         1026048    42051583    20512768   8e  Linux LVM
   /dev/sdb3        42051584   976707583   467328000   8e  Linux LVM
   ```

   Additional entries for the file system (sdb4, sdb5) could be possible. For example:

   ```
   Disk /dev/sdb: 598.9 GB, 598879502336 bytes
   255 heads, 63 sectors/track, 72809 cylinders, total 11696828 sectors
   Units = sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disk identifier: 0x930a8a0e


      Device Boot      Start         End      Blocks   Id  System
   /dev/sdb1   *        2048     1026047      512000   83  Linux
   /dev/sdb2         1026048     2050047      512000   83  Linux
   /dev/sdb3         2050048    43075583    20512768   8e  Linux LVM
   /dev/sdb4        43075584  1169686527   563305472    5  Extended
   /dev/sdb5        43077632  1169686527   563304448   8e  Linux LVM
   ```

   You will need to delete the any partitions on the RAID 1 volume and the RAID 5 volume (if applicable). This process will assume “sdb” is the RAID 1 and “sdc” is the RAID 5.

10. Use the RHEL fdisk utility to select the sdb volume:

    ```
    fdisk /dev/sdb
    ```

11. Type: **`p`** to print the current filesystem partition table. This will show you a similar output as the fdisk –cul command you used earlier.
12. Type: **`d`** to begin deleting the partitions.
13. You will be prompted to specify the partition to delete. For example: **`1`**

    ```
    Partition number (1-4): 1
    ```

14. Repeat the above two steps to delete the remaining “sdb” partitions.
15. Once complete, type **`p`** to print the partition table again. An empty partition table should look like the following:

    ```
    Device Boot      Start         End      Blocks   Id  System
    ```

16. Type: **`w`** to write the changes to the partition table and exit the utility.
17. If you have a RAID 5 volume, repeat this process by specifying the RAID 5 “sdc” partition:

    ```
    fdisk /dev/sdc
    ```

18. Repeat the above steps and type **`w`** to write the changes to the partition table and exit the utility.
19. Verify that the partitions on sdb and sdc (if applicable) were successfully removed using the RHEL fdisk utility:

    ```
    fdisk -cul
    ```

20. Reboot the server by selecting CTRL-ALT-DEL. You will again boot from the USB Installation drive. The correct partitions and filesystems will be created automatically during the installation.

Proceed to “MCS Software Deployment” on page 64.

MCS Software Deployment

This process will install both RHEL and MCS from the MCS Installation USB drive.

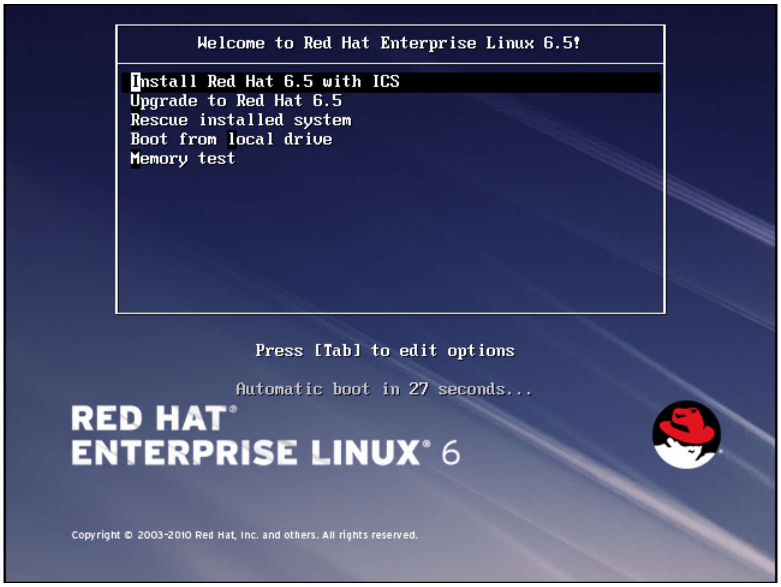
To install RHEL and MCS from the USB installation drive:

1. Ensure the MCS Installation USB drive is connected to the server and either boot or reboot the server if it is already powered-on.

For HP installs, an error message may appear: "[Firmware Bug]: the BIOS has corrupted hw-PMU resources". This error can be ignored.

If you are installing MCS on an HP ProLiant Gen9 server and you get a black screen on boot, you might need to alter a particular BIOS setting. Select Advanced Options > Video Options from the system's BIOS/Platform Configuration (RBSU) menu and change the embedded video connection setting from "auto" to "always on".

2. Wait for the RHEL Welcome screen to appear.



```
Welcome to Red Hat Enterprise Linux 6.5!

Install Red Hat 6.5 with ICS
Upgrade to Red Hat 6.5
Rescue installed system
Boot from local drive
Memory test

Press [Tab] to edit options

Automatic boot in 27 seconds...
```

Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

It has been reported that under some circumstances the installation bypasses the RHEL Welcome screen. This will not affect the install process. The correct installation choice is always selected by default.

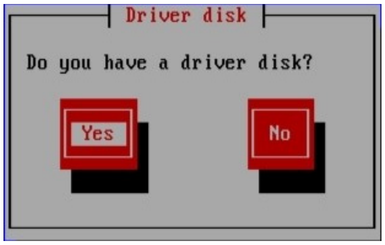
3. If you are installing on an HP ProLiant Gen9 server, install the RHEL driver to enable RHEL support for the storage controller before proceeding:

   a. Press the Esc key to open the RHEL boot shell.

   b. At the boot shell, type the following:

   ```
   linux dd
   ```

c. In the dialog that appears, confirm that you have a driver disk.



Driver disk

Do you have a driver disk?

d. The installer may prompt you to specify the location of the update. Select the device name indicating the MCS Installation USB drive (e.g sda). Similarly specify the partition on the device (e.g. sda1).

e. Select the driver and select OK:

```
z_dd-hpsa-18216-x86_64.iso
```

f. When prompted for more drivers, select No.

The driver is updated, and the installation process continues as described below.

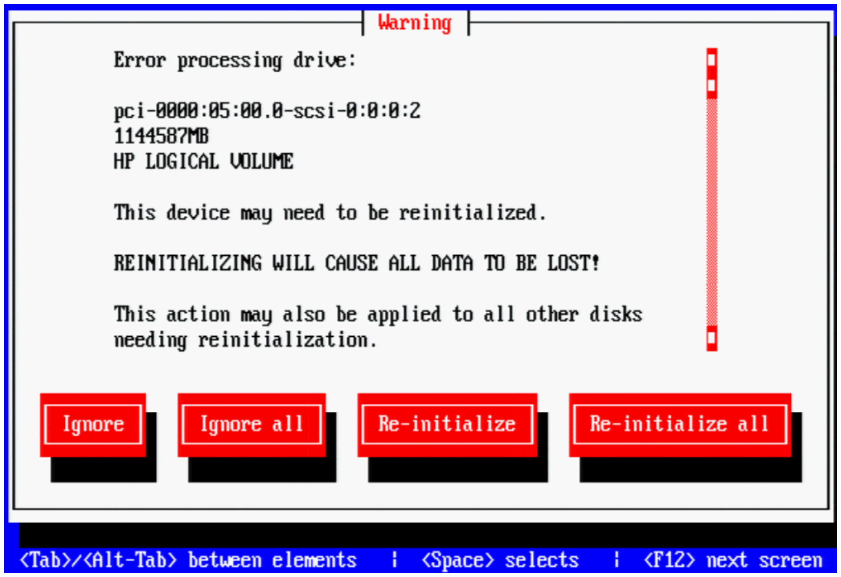
4. Select "Install Red Hat with ICS" to install a new MCS and press Enter.

If you are upgrading your system, do not use the "Upgrade" option. For upgrade instructions, see the "MediaCentral Platform Services Upgrade Guide".

The RHEL and MCS packages are installed—this takes about 20 minutes.

If you see an "`Unable to download kickstart file`" message, it means that the installation program could not locate the kickstart file on the "sda" partition. Linux might automatically assign the sda partition to an SD card slot or a KVM with "virtual media" capability. To resolve the issue, temporarily disable the device that is using the sda partition name. If you are accessing the server through a KVM, unplug the KVM and connect an external monitor and USB keyboard directly to the server.

5. If you just created the RAIDs a warning screen appears indicating a device (i.e. the RAIDs) needs to be reinitialized. This is normal. Select Re-Initialize All.

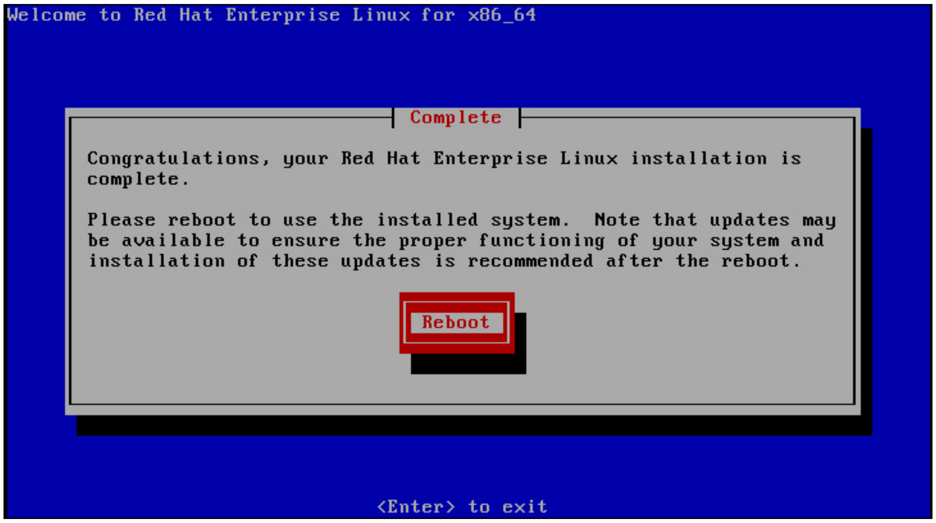


Warning

```
Error processing drive:

pci-0000:05:00.0-scsi-0:0:0:2
1144587MB
HP LOGICAL VOLUME

This device may need to be reinitialized.

REINITIALIZING WILL CAUSE ALL DATA TO BE LOST!

This action may also be applied to all other disks
needing reinitialization.
```

Ignore
Ignore all
Re-initialize
Re-initialize all
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

6. When the installation process is complete, you are prompted to reboot. **DO NOT REBOOT before removing the MCS Installation USB drive**.



```
Welcome to Red Hat Enterprise Linux for x86_64

Complete

Congratulations, your Red Hat Enterprise Linux installation is
complete.

Please reboot to use the installed system.  Note that updates may
be available to ensure the proper functioning of your system and
installation of these updates is recommended after the reboot.
```

If you reboot without removing the USB drive the server will reboot from the USB drive again and re-launch the installer.

If you pressed Enter by mistake, remove the USB drive as quickly as possible (before the system boots up again). If this is not possible, you might need to perform the installation again.

7. Once the MCS Installation USB drive is removed, press Enter to reboot the server.

Booting RHEL for the First Time

Like many operating systems, when you boot RHEL for the first time, you will be asked to provide some basic information. A “first boot” of RHEL causes the Text Mode Setup Utility screen to appear, providing access to system configuration menus.

If needed, the setup utility can be access from Linux at any time by typing: **`setup`**

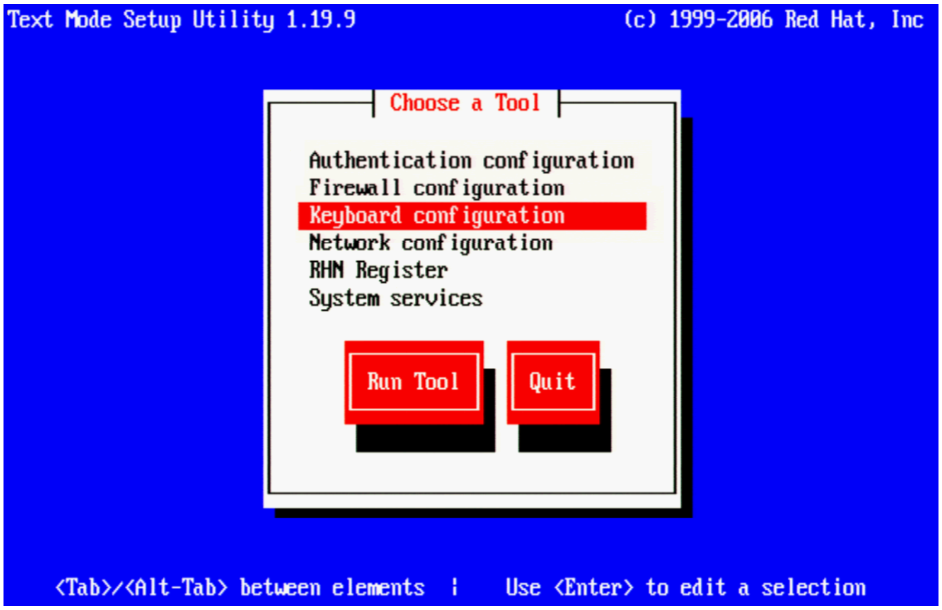
Verifying the Keyboard configuration

Some MCS software components depend on the language for RHEL being set to English. This is done automatically by the MCS installation scripts. Do not change the input language afterwards.

Selecting a language for the keyboard is different from the language selected for RHEL. While selecting a different language for the keyboard is supported, the RHEL language must remain as English.

To adjust the input language:

1. From the Choose a Tool menu, arrow down to select “Keyboard Configuration” and press Enter.



```
Text Mode Setup Utility 1.19.9                    (c) 1999-2006 Red Hat, Inc

   <Tab>/<Alt-Tab> between elements   |   Use <Enter> to edit a selection
```

2. In the Keyboard Selection menu, use the arrows to select the appropriate language for your keyboard.
3. Press the Tab key to focus on the OK button and press Enter.
4. Press the Tab key to focus on the Quit button and press Enter.

Changing the root Password

The RHEL installation script configures a default password for the root user (the Linux user with administrator privileges). For security reasons, it is strongly suggested that you change the password for the root user at the earliest opportunity.

To change the root password:

1. Log in a the Linux prompt

   Default user name: root

   Default password: Avid123

2. While logged in as the root user type the Linux change password command:

   ```
   passwd
   ```

3. Follow the prompts to change the password.

   If you do not enter a strong password, RedHat will warn you that the password is bad. This could be because you have entered a password based on a word in the dictionary. While this warning can be ignored, Avid suggests using strong passwords.

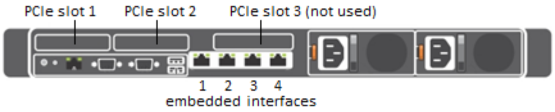
Network Configuration

MCS servers support both static and dynamic (DHCP) IP addressing. Static addressing is the Avid recommended method for any MCS server and is a requirement for any MCS cluster deployment.

Normally, on a server with multiple network interfaces (i.e. Ethernet connectors), each interface has its own IP address. However, MCS servers in Interplay MAM can benefit from port bonding (a.k.a. teaming), in which several network interfaces appear as a single IP address. Port bonding is supported in MCS for MAM deployments only. For more information, see "Port Bonding for Interplay MAM" on page 269.

Under the Linux operating system, every physical network connector, called an *interface* in Linux, has a name. By default, when installing RHEL, the installer scans the NIC cards in the machine and labels the interfaces it finds, in the order it finds them.

- HP Servers: Each interface in an HP server is labeled "ethx", where 'x' is an incremental number starting with zero. Example: eth0, eth1, eth2 and so on. This naming convention is true for both onboard and add-in (PCIe) network adapters.
- Dell Onboard: The Dell onboard interfaces are similar to the HP in that each interface is labeled as "emx", where 'x' is an incremental number starting with one. Example: em1, em2, em3 and so on. This naming convention only applies to the onboard 1 Gb interfaces.
- Dell PCIe Slots: The PCIe slots in a Dell are labeled as "p1p1" (slot 1) and "p2p1" (slot 2). If you are using a 10 Gb network adapter in the Dell, it will be assigned one of these labels; depending upon where you added the card (either slot is acceptable).



This installation guide will use "eth0 as the default example for many commands. If you are using a Dell server, make sure to substitute "eth0"with the correct interface name for your deployment. In general on a Dell, these should be "em1" or "p1p1".

To obtain a list of the NICs installed in your system, enter the following in a Linux command prompt:

```
lspci | grep net
```

Verify DNS

The Avid MCS implementation on RHEL is not configured to automatically register in DNS. Work with your on-site IT Department to manually enter each MCS server in both Forward and Reverse DNS.

If you will be configuring an MCS cluster, the cluster's virtual IP and hostname should also be entered in DNS.

From a Windows system, the "nslookup" command can be used in a command prompt to check the DNS records directly.

Identifying NIC Interfaces and Connecting the Network Cable

RHEL provides a simple means for visually identifying the NIC ports on a server, whether they are active or not. The `ethtool` command can be used to cause ports to blink for a pre-determined amount of time.

To visually identify a NIC interface:

1. Use the Linux ethtool command, identify your primary network interface by causing it to blink for 60 seconds:

   ```
   ethtool --identify <interface name> 60
   ```

   Where <*interface name*> is the name of the interface you want to identify.

   - For HP servers, this is: eth0
   - For Dell servers using a 1 Gb connection, this is: em1
   - For Dell servers using a 10 Gb connection, this is: p1p1 or p2p1

   Example: `ethtool --identify eth0 60`

   Note the use of the double-dash in the identify command. In Linux, single dashes verses double-dashes distinguish *options* from *arguments*. A double-dash often precedes a word (i.e. human readable) option.

2. Connect your network cable at this time.

   a. If you are on a Dell server, connect your network cable to the interface that flashed for “em1”, “p1p1” or “p2p1”.

      Skip to “Configuring the Hostname and Static Network Route” on page 72.

   b. If you are on an HP server and will be connecting through a 1 Gb connection to a supported onboard NIC, connect your network cable to the interface that flashed for “eth0”.

      Skip to “Configuring the Hostname and Static Network Route” on page 72.

   c. If you are on an HP server and will be connecting through 10 Gb connection, connect the fibre cable to the PCIe card.

      Proceed to “(HP Only) Verifying the NIC Interface Name” on page 69.

   d. If you are on an HP server and will be connecting through a 1 Gb connection to an add-in 1 Gb NIC, “eth0” may or may not have flashed on that card. If the above command made “eth0” flash on the add-in card, connect your cable to the port that flashed. If the above command made “eth0” flash on the onboard adapter, connect the network cable to the first port (far left) of the add-in card and repeat the identify command to determine the name of the port you are connected to (you will need this information in the following step).

      Proceed to “(HP Only) Verifying the NIC Interface Name” on page 69.

3. If needed, repeat the above to identify additional ports.

(HP Only) Verifying the NIC Interface Name

In an HP server, Avid assumes that interface “eth0” will be used. Since all interfaces in an HP server are named “ethx”, additional steps need to be taken to ensure “eth0” is used.

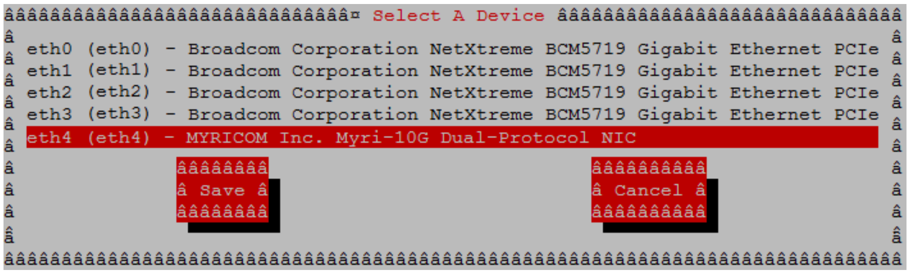
To verify the NIC interface name:

1. Enter the RHEL Configuration screen by typing the following at the command prompt:

   ```
   setup
   ```

2. From the Choose a Tool menu, select Network Configuration and press Enter.
3. From the Network Configuration menu, select Device Configuration and press Enter.

   A list of NIC cards contained in the server enclosure appears.



```
eth0 (eth0) - Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe
eth1 (eth1) - Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe
eth2 (eth2) - Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe
eth3 (eth3) - Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe
eth4 (eth4) - MYRICOM Inc. Myri-10G Dual-Protocol NIC
```

4. Make note of the name associated with your interface. If necessary, use the arrow keys to move up and down the list.

   In the above example, a 10 Gb card has been placed in the server. It is currently assigned “eth4”, but we will want to change that to “eth0”.
5. Note the name assigned to the interface of interest (e.g. eth0, eth1, eth*n*).
6. Perform the actions required at each menu (Cancel, Quit, Exit, etc.) to return to the Linux prompt.

(HP Only) Swapping NIC Interface Names

If your interface of interest was not already named “eth0”, you must rename it. You must also rename the NIC interface currently using the name “eth0”.

To rename the network interface:

1. Edit the network script where persistent names are assigned to network interfaces:

   ```
   vi /etc/udev/rules.d/70-persistent-net.rules
   ```

A server with just one installed NIC card does not have a 70-persistent-net.rules file by default. If the file is missing for any reason, it can be created using the following command:

```
udevadm trigger --subsystem-match=net
```

The contents of the file might look similar to the following:

```
# PCI device 0x14e4:0x1657 (tg3)

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="ac:16:2d:74:1b:58", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth0"
# PCI device 0x14e4:0x1657 (tg3)

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="ac:16:2d:74:1b:59", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth1"

# PCI device 0x14e4:0x1657 (tg3)

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="ac:16:2d:74:1b:5a", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth2"
```

```
# PCI device 0x14e4:0x1657 (tg3)

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="ac:16:2d:74:1b:5b", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth3"

# PCI device 0x14c1:0x0008 (myri10ge)

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="00:60:dd:45:14:50", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth4"
```

Note that in this example, a 10Gb Myricom card has been added to the system and has been designated as “eth4”. In this scenario, you must swap the names for “eth0” and “eth4” so that the Myricom board is used as the primary network adapter.

2. Identify the lines in the file that correspond to the interface you want to name eth0 and the one already using the name.

   Use the arrow keys on the keyboard to navigate the file.

3. Press the **A** key to begin editing the file.
4. Change NAME="eth*X*" (e.g. *eth1*, *eth2*, etc.) to the following:

   ```
   NAME="eth0"
   ```

5. Locate the line corresponding to the interface that was assigned to “eth0” and rename it:

   ```
   NAME="ethX"
   ```

   Where “*X*” is the number you removed in step 4 (e.g. *eth1*, *eth2*, etc.); that is, swap the names.

6. Save and exit the vi session. Press **<ESC>** and type: **:wq**

(HP Only) Removing the MAC Address Hardware References

In addition to renaming the network interfaces, you must also remove the hardware references – generally known as MAC addresses – from the affected NIC interface configuration files.

For each card where you renamed a network interface, edit the corresponding interface configuration file and remove the hardware identifier. If you do not, Linux will override your changes and reassign the original interface names on the next system reboot (or restart the Linux network services).

To remove the MAC address:

1. Using the Linux text editor, vi, open the interface configuration file for one of the renamed interfaces (e.g. ifcfg-eth0):

   ```
   vi /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

   In Linux, each network interface has its own configuration file.

2. Locate the line containing the hardware identifier. It has the following form:

   ```
   HWADDR = 00:00:00:00:00:00
   ```

3. Position the cursor on the HWADDR line and press “dd” to remove it. That is tap the lower case letter D twice.
4. Save and exit the vi session. Press **<ESC>** and type: **:wq**
5. Repeat the above steps for the other NIC interface you renamed (e.g. *ethX*).

6. Once you have finished removing the hardware references for both the renamed NIC interfaces, reboot the server to restart the network services and make the effects permanent:

   ```
   reboot
   ```

   The MAC addresses refresh automatically after the reboot.

7. Once the system has rebooted, log back into RHEL.

Changing the contents of the /etc/udev/rules.d file requires a reboot rather than simply restarting network service.

Configuring the Hostname and Static Network Route

This process assumes that the configuration of a static IP address is desired.

To configure the system hostname and IP address:

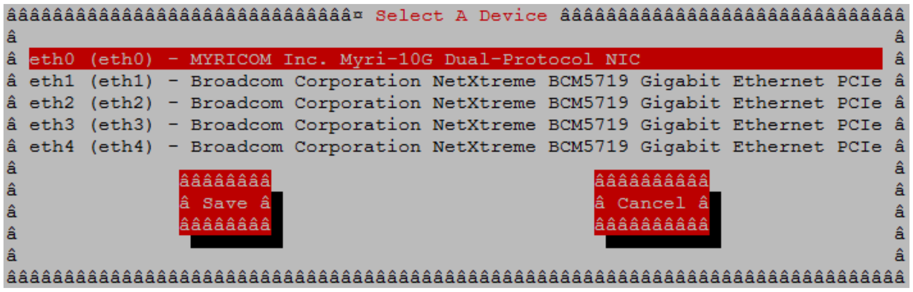
1. Enter the RHEL Configuration screens by typing the following at the command prompt:

   ```
   setup
   ```

2. From the Choose a Tool menu, select Network Configuration and press Enter.

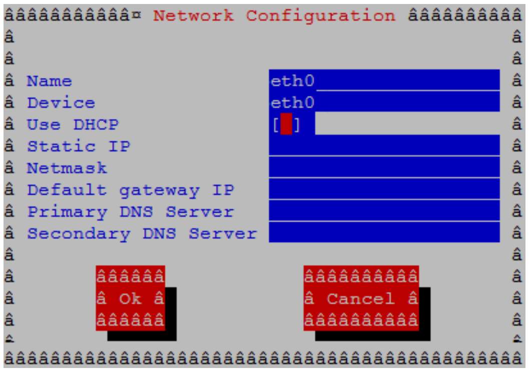
3. From the Network Configuration menu, select Device Configuration and press Enter.

   A list of network interfaces appears.



```
âââââââââââââââââââââââââââââââ¤ Select A Device ââââââââââââââââââââââââââââââ
â                                                                             â
â eth0 (eth0) - MYRICOM Inc. Myri-10G Dual-Protocol NIC                       â
â eth1 (eth1) - Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe  â
â eth2 (eth2) - Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe  â
â eth3 (eth3) - Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe  â
â eth4 (eth4) - Broadcom Corporation NetXtreme BCM5719 Gigabit Ethernet PCIe  â
â                                                                             â
â              ââââââââ                             ââââââââââ                â
â              â Save â                             â Cancel â                â
â              ââââââââ                             ââââââââââ                â
â                                                                             â
âââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââââ
```

4. Use the arrow keys to locate the primary interface (eth0, em1 or p1p1) and press Enter to view its details.



```
ââââââââââââ¤ Network Configuration ââââââââââ
â                                           â
â                                           â
â Name                  eth0                â
â Device                eth0                â
â Use DHCP              [ ]                 â
â Static IP                                 â
â Netmask                                   â
â Default gateway IP                        â
â Primary DNS Server                        â
â Secondary DNS Server                      â
â                                           â
â       ââââââ           ââââââââââ         â
â       â Ok â           â Cancel â         â
â       ââââââ           ââââââââââ         â
â                                           â
ââââââââââââââââââââââââââââââââââââââââââââââ
```

If you configured port bonding for an Interplay MAM integration, your primary interface may be called "bond0". For more information on port bonding, see "Port Bonding for Interplay MAM" on page 269.

5. The software installs with a default Static IP of 127.0.0.2 and a default Netmask of 255.0.0.0. Replace the following fields with customized values for your site:

   - Static IP address
   - Netmask (Subnet)
   - Default gateway IP
   - Primary DNS server
   - Secondary DNS server (if applicable)

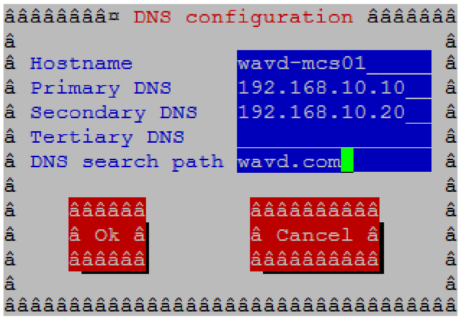
All MCS servers in a cluster must be in the same subnet.

6. Arrow or Tab down to the OK button and press Enter.

   You are returned to the list of network interfaces.

7. Select Save and press Enter.

8. From the Choose a Tool menu, select DNS Configuration and press Enter.



```
âââââââââ¤ DNS configuration âââââââ
â                                 â
â Hostname         wavd-mcs01____ â
â Primary DNS      192.168.10.10__ â
â Secondary DNS    192.168.10.20__ â
â Tertiary DNS                    â
â DNS search path  wavd.com       â
â                                 â
â    ââââââ        ââââââââââ     â
â    â Ok â        â Cancel â     â
â    ââââââ        ââââââââââ     â
â                                 â
âââââââââââââââââââââââââââââââââââ
```

9. Enter the following information for the DNS Configuration:

   - Hostname

     Specify the short hostname only (e.g. wavd-mcs01) and not the fully qualified domain name (FQDN) (e.g. wavd-mcs01.wavd.com) in this field.

Hostnames should comply with “RFC 952” and “RFC-1123” standards. Avid recommends keeping host names under 15 characters to maintain backwards compatibility with older systems. The only “special character” allowed in a hostname is a dash “ - ”. Underscores are not allowed.

For more information on RFC specifications, see https://ietf.org/rfc.html. For additional information on host name restrictions in Microsoft Windows domains, see https://technet.microsoft.com/en-us/library/cc959336.aspx.

   - Primary DNS server
   - Secondary DNS server (if applicable)
   - Tertiary DNS server (if applicable)
   - DNS search path

10. Select Save & Quit. Press Enter.

11. Select Quit. Press Enter.

Verifying the hosts File Contents

The *hosts* file is used by the operating system to map hostnames to IP addresses. It allows network transactions on the computer to resolve the right targets on the network when the instructions carry a “people-friendly” hostname (e.g. wavd-mcs01) rather than an IP address (e.g. 192.xxx.xxx.xxx.xxx). Querying and waiting for a response from a DNS server can be slow due to network latency. The hosts file assists in quickly resolving hostnames to IPs which is particularly important for clustered configurations.

By default the hosts file on a computer resolves the machine’s own IP address to localhost. In this step, you verify the content of the hosts file, and remove any extra entries, if present. In addition, since the active hosts file can be reset to its default configuration when a server fails or is rebooted you also verify the system default hosts file.

To configure the local hosts file:

1. Using the Linux *vi* editor, open the active hosts (/etc/hosts) file for editing:

   `vi /etc/hosts`

   It should look similar to the following:

   ```
   127.0.0.1  localhost  localhost.localdomain  localhost4  localhost4.localdomain4
   ::1        localhost  localhost.localdomain  localhost6  localhost6.localdomain6
   ```

   In this example, the default IP address of 127.0.0.1 is mapped to various forms of localhost, for both ipv4 and ipv6 systems.

   In some cases, the entries include an explicit call-out of the computer’s own host name (e.g. wavd-mcs01):

   ```
   127.0.0.1  localhost  localhost.localdomain  localhost4  localhost4.localdomain4  wavd-mcs01
   ::1        localhost  localhost.localdomain  localhost6  localhost6.localdomain6  wavd-mcs01
   ```

   In a cluster the explicit call-out of the computer’s own host name is particularly problematic. If this entry remains unaltered, another node querying “wavd-mcs01” for its IP address would receive “127.0.0.1” in response. The querying node would send messages to itself instead of to the real “wavd-mcs01”, and clustering would not function normally.

   If the computer’s host name (e.g. wavd-mcs01) is present in either line, remove the entry:

   ```
   127.0.0.1  localhost  localhost.localdomain  localhost4  localhost4.localdomain4
   ::1        localhost  localhost.localdomain  localhost6  localhost6.localdomain6
   ```

2. If you are configuring an MCS cluster, add the IP addresses, FQDN and hostnames of each of the cluster nodes and the virtual cluster.

For a four node cluster, for example, you would add five lines similar to the following:

```
127.0.0.1      localhost             localhost.localdomain  localhost4   localhost4.localdomain4
::1            localhost             localhost.localdomain  localhost6   localhost6.localdomain6
192.168.10.50  wavd-mcs.wavd.com     wavd-mcs
192.168.10.51  wavd-mcs01.wavd.com   wavd-mcs01
192.168.10.52  wavd-mcs02.wavd.com   wavd-mcs02
192.168.10.53  wavd-mcs03.wavd.com   wavd-mcs03
192.168.10.54  wavd-mcs04.wavd.com   wavd-mcs04
```

When adding the node data, make sure to enter the IP address, FQDN and short hostname – in that order. If you enter the information in the wrong order, the Linux “hostname” and “hostname -f” commands could reply with invalid responses.

It is a good idea to declare the nodes in the hosts file in order of latency, ascending. Run a ping command to each node and add the lines to the file in order of the ping return. For example, if node-2 returns a ping after 30ms and node-3 after 20ms, put in the line for node-3 before node-2.

3. Save and exit the vi session. Press **<ESC>** and type: **`:wq`**

4. If you made changes, verify that the system default hosts file reflects the changes.

   ```
   cat /etc/sysconfig/networking/profiles/default/hosts
   ```

   If necessary, *vi* can be used to edit the file to match the changes you made to the master hosts file.

Verifying the Contents of resolv.conf and nsswitch.conf

The `resolv.conf` file contains the DNS and domain information that you entered through the Linux Setup Utility.

Avid adjusts the nsswitch.conf file to instruct RHEL to prefer the local hosts file over DNS. In cluster configurations, this ensures that there is no latency when attempting to discover the cluster nodes.

Before enabling the network interface, it is best practice to verify that the information contained in these files is correct.

To verify the resolv.conf file:

1. Use the Linux cat command to display the contents of the (resolv.conf) file and verify its contents:

   ```
   cat /etc/resolv.conf
   ```

   The DNS servers and DNS search path should be present in the file.

   If necessary, the *vi* editor can be used to add one or more additional search domains. The search list is limited to six domains with a total of 256 characters. The file should look something like:

`nameserver <IP address of server1>`	(Primary DNS server)
`nameserver <IP address of server2>`	(Secondary DNS server)
`search domain1.com domain2.com`	(multiple domain names separated by a single space or tab can be entered)

2. Delete any backup resolver configuration (resolv.conf.save) file that might have been automatically created by the OS:

   ```
   rm /etc/resolv.conf.save
   ```

If you do not delete the `.save` *file, Linux will overwrite the changes you just made on the next reboot.*

To verify the nsswitch.conf file:

1. Review the contents of the nsswitch.conf file using the cat command:

   ```
   cat /etc/nsswitch.conf | grep hosts
   ```

   The system outputs the lines containing the string “hosts”, similar to the following:

   ```
   #hosts: db files nisplus nis dns
   hosts:  files dns
   ```

   In the second line, ensure that the word “files” comes before the word “dns”.

2. If “files” does not appear before “dns”, use the vi editor to reverse the priority order.

Ensuring the NIC Interface Comes Up at System Startup

In this step, you must verify that the primary network interface is configured to be enabled when the system boots.

To verify the network interface boot setting:

1. Using the Linux *vi* editor, open the *eth0* interface configuration file for editing:

   ```
   vi /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

If you are on a Dell server, remember to substitute “em1”, “p1p1” for “eth0”.

2. When you open the file for editing, it should look something like this:

   ```
   DEVICE=eth0
   HWADDR=00:60:dd:45:15:11
   TYPE=Ethernet
   UUID=
   ONBOOT=yes
   NM_CONTROLLED=no
   DHCP_HOSTNAME=’$HOSTNAME’
   BOOTPROTO=none
   IPADDR=192.169.10.51
   NETMASK=255.255.255.0
   DNS1=192.169.10.10
   DNS2=192.169.10.20
   GATEWAY=192.168.10.1
   USERCTL=no
   IPV6INIT=no
   ```

3. Ensure that the ONBOOT entry is set to “yes”. If it is not, the interface will not be active after rebooting the server.

4. Save and exit the vi session. Press **<ESC>** and type: **`:wq`**

5. Reboot the MCS server:

   ```
   reboot
   ```

You are asked to reboot at this time to ensure that all networking changes are active and the system comes up as expected. If you do not reboot, some of the steps in the next procedure will fail.

6. Once the system has rebooted, log back into RHEL.

Verifying Hostname, Network and DNS Connectivity

Before continuing, take a moment to verify that the server's hostname responds as expected and that network connectivity is now established.

To verify the hostname:

1. Verify the short hostname. In the RHEL command prompt, type:

   ```
   hostname
   ```

   The short hostname (e.g. wavd-mcs01) should be printed to the screen.

2. Verify the fully qualified domain name (FQDN). In the RHEL command prompt, type:

   ```
   hostname -f
   ```

   The fully qualified hostname (e.g. wavd-mcs01.wavd.com) must be printed to the screen. If the command replies with the short hostname, there is a configuration error.

If you do not receive the expected output, verify your hosts file and the resolv.conf file.

To verify network connectivity:

1. Use the ping command to verify connectivity to your network gateway address:

   ```
   ping -c 4 <gateway IP address>
   ```

   "ping" is the command. "-c 4" is the count of how many times the ping command is issued. If you do not specify a count, ping will continue forever. In that event, press CTRL-C to stop the ping. For example:

   ```
   [root@wavd-mcs01 ~]# ping -c 4 192.168.10.1
   PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
   64 bytes from 192.168.10.1: icmp_seq=1 ttl=255 time=0.362 ms
   64 bytes from 192.168.10.1: icmp_seq=2 ttl=255 time=0.330 ms
   64 bytes from 192.168.10.1: icmp_seq=3 ttl=255 time=0.302 ms
   64 bytes from 192.168.10.1: icmp_seq=4 ttl=255 time=0.804 ms
   ```

2. Now use the ping command to test the connection to host servers in your network. Examples of host servers could be: Interplay Production Engines, Avid System Directors, iNEWS servers, etc. This not only tests the connection to the host server, but also verifies DNS.

   ```
   ping -c 4 <hostname>
   ```

3. Repeat the ping test; this time by pinging the host servers by IP address.

Now that you have configured and verified the connection to the network, you can now switch to using an indirect method for configuring the server. For more information refer back to "Accessing the MCS Server(s)" on page 21.

Configuring Access for External Systems

External systems such as Interplay Production and Interplay MAM that have installed the Avid Connectivity Toolkit must be added to a configuration file on the MCS server. This configuration file builds a “whitelist” of systems allowed to connect to the MediaCentral BAL (Bus Access Layer) for enhanced security. Any system running the Avid Connectivity Toolkit that is not included in this file might encounter errors when connecting to the Bus.

To enable access for external systems:

1. Using the Linux text editor, vi, open the configuration file for editing:

   ```
   vi /etc/sysconfig/avid-acs-gateway
   ```

2. Locate the following line in the configuration file:

   ```
   #export ACS_SECURITY_FULL_TRUST_IPV4_MASK_LIST="127.0.0.1/25;"
   ```

3. Activate (uncomment) this line by removing the “#” in front of it.
4. Add the IP address of the any external system to this line, followed by a semicolon:

   ```
   export ACS_SECURITY_FULL_TRUST_IPV4_MASK_LIST=”127.0.0.1/25;<ip>;”
   ```

   External systems include:

   - Interplay Production: Enter the IP address of any system that has the Avid Connectivity Toolkit installed. The Toolkit is shipped with the Interplay Production software package and requires a separate installation. The Toolkit is not automatically installed.
   - Interplay MAM: Enter the IP addresses of all MAM servers that are to be connected to MediaCentral Platform Services (including fail-over servers).
   - Avid iNEWS: Enter the IP address(es) of any local iNEWS server(s) that are running the CTC service. You are not required to list all iNEWS servers in a Community configuration.

   Each entry must be followed by a semicolon. In the following example, a single IP address of 192.168.50.98 is added to the configuration:

   ```
   export ACS_SECURITY_FULL_TRUST_IPV4_MASK_LIST="127.0.0.1/25;192.168.50.98;"
   ```

   Notice the required quotation marks that enclose the string. The 127.0.0.1/25 entry is a reference to the local MCS server.

Do not remove 127.0.0.1/25 from the configuration. This address is required for MediaCentral Platform Services to operate.

   If you have a group of IP addresses that need to connect to MCS, a range can be substituted for a list of individual IP addresses. When specifying a range of addresses, you must add a netmask after the IP range. In the following example, the single server at 192.168.50.98 and all IP addresses in the 192.168.100.x range are allowed to connect to MCS:

   ```
   export ACS_SECURITY_FULL_TRUST_IPV4_MASK_LIST="127.0.0.1/
   25;192.168.50.98;192.168.100.0/24;"
   ```

   In this example, a netmask of /24 has been used with the 192.168.100.0 IP range.

5. Save and exit the vi session. Press <ESC> and type: **:wq**
6. If you are configuring multiple systems in a cluster, complete the above steps on all nodes.
7. Restart the avid-acs-gateway service to enable the change:

   ```
   service avid-acs-gateway restart
   ```

If you are completing this process for a fully configured cluster, restart the cluster resource associated with the avid-acs-gateway service. Complete this step once from any cluster node:

```
crm resource restart AvidGatewayEverywhere
```

For a fully configured cluster, use the Cluster Resource Monitor to review the status of the cluster and clear any fail-counts.

Configuring Date and Time Settings

Ensuring that the date, time and time zone are correct on each MCS server is critical to a successful implementation. This process will walk you through configuring the above values as well as setting a Network Time Protocol (NTP) source for continued time synchronization.

If you do not have an NTP server already configured, see your local IT Department about creating one prior to continuing with this process. Maintaining time synchronization between MCS servers and host systems (Avid shared storage, Interplay Production, etc) is critical. Maintaining time synchronization between nodes in an MCS cluster configuration is particularly critical.

Setting the Time Zone

When using the MCS Installation USB drive to install RHEL, the kickstart file automatically sets the time zone to America/New_York. If this zone is not correct for your configuration, you must complete this process. If you are already in this time zone, you can skip to the process for Syncing the System Clock.

To adjust the timezone:

1. Verify the current time zone by viewing the contents of the Linux “clock” file:

   ```
   cat /etc/sysconfig/clock
   ```

2. List the contents of the directory containing RHEL time zone information:

   ```
   ls /usr/share/zoneinfo
   ```

   A list of time zone regions is presented. For example, US time zones are located in /usr/share/zoneinfo/US (standard US time zones), European time zones are located in /usr/share/zoneinfo/Europe, and so on...

3. List the contents of the directory that are specific to your location:

   ```
   ls /usr/share/zoneinfo/<location>
   ```

   For example:

   ```
   ls /usr/share/zoneinfo/US
   ```

4. Make note of the time zone name that relates to your installation location.

5. Edit the clock file to reflect the correct time zone for your installation:

   ```
   vi /etc/sysconfig/clock
   ```

   Example: Replace `zone="America/New_York"` with `zone="US/Pacific"`

6. Save and exit the vi session. Press **<ESC>** and type: **:wq**

7. Create the symbolic link RHEL needs to make use of the new time zone information:

   ```
   ln -sf /usr/share/zoneinfo/<yourzone> /etc/localtime
   ```

   In the above command, *<yourzone>* is the path you entered in the clock file (e.g. US/Pacific).

Creating a symbolic link is more robust than copying. For example, the files in /usr/share/zoneinfo contain daylight saving time (DST) information. A symbolic link allows your system to automatically accommodate changes to DST practices that might arise in the future. Such changes would be propagated through RHEL updates to the /usr/share/zoneinfo files.

8. Verify the settings using the date command:

   ```
   date
   ```

   The local time and time zone should now be shown.

Synchronizing the System Clock

In this step you set the Network Time Protocol (NTP) daemon to automatically synchronize the system clock with an NTP time server every 30 minutes. This is done by creating a job for the Linux cron utility. The cron job runs the NTP daemon, ntpd.

Setting up ntpd to run as a service at startup is also a possibility. However, some consider it a security risk to run ntpd in "continuous" mode. The technique shown here keeps the system clock synchronized while minimizing exposure to risk by causing ntpd to exit after it fetches the correct time.

The use of the "iburst" option within the cron job is not recommended. This feature produces very rapid time shifts and can lead to synchronization problems.

To synchronize the system clock:

1. Verify the current date and time with the Linux date command:

   ```
   date
   ```

2. This process will verify connectivity to the NTP server. Change the date and time so that the clock is **10 minutes** behind the correct time of day.

   ```
   date MMDDHHmmYYYY
   ```

Avid suggests creating a 10 minute offset. If you create an offset of more than 17 minutes, Linux sees this as a more serious problem and may not update the clock.

3. Check the status of the ntpd service:

   ```
   service ntpd status
   ```

   If the service is running, stop the service:

   ```
   service ntpd stop
   ```

4. Verify that the NTP server of interest is reachable by querying it:

   ```
   ntpdate -q <ntp_server_address>
   ```

   Example output:

   ```
   server 192.168.10.25, stratum 3, offset 468.746036, delay 0.02585
   1 Jan 13:05:00 ntpdate[7554]: step time server 192.168.10.25 offset
   468.746036 sec
   ```

5. Edit the NTP configuration (ntp.conf) file:

   ```
   vi /etc/ntp.conf
   ```

6. Scroll down to the section of the file that details the NTP servers and place a '#' symbol in front of any existing NTP servers to comment them out. For example:

   ```
   # server 0.rhel.pool.ntp.org
   # server 1.rhel.pool.ntp.org
   # server 2.rhel.pool.ntp.org
   ```

7. Update the file with the NTP information for your configuration. Updated example:

   ```
   # server 0.rhel.pool.ntp.org
   # server 1.rhel.pool.ntp.org
   # server 2.rhel.pool.ntp.org
   server 192.168.10.25 prefer
   server 192.168.10.26
   ```

   If you are configuring two or three NTP servers, add the "prefer" option to the first NTP server. This configures the first server as the primary and eliminates the possibility of the client fluctuating between time sources. If the primary NTP server is offline, the next NTP server in the list is used. If you are using four or more time servers, do not use the "prefer" option.

8. Save and exit the vi session. Press **<ESC>** and type: **:wq**
9. Set up a cron job by creating a new file containing instructions for cron:

   ```
   vi /etc/cron.d/ntpd
   ```

10. Add the following text which includes the instructions for the cron job:

    ```
    0,30 * * * * root /usr/sbin/ntpd -q -u ntp:ntp
    ```

    The command above instructs cron to:

    - Run the cron job every 30 minutes as root.

      "0,30" is a comma-separated list (i.e. run at 0 minutes and 30 minutes). "*" is a special list indicating every value in the list (i.e. every hour, every day of the month, every month, every day of week).

    - The job is /usr/sbin/ntpd
    - The -q switch tells ntpd to exit after it sets the system clock
    - The -u switch tells Linux to run the job as user *ntp*, in user group *ntp*

    The general form of the cron command is the following:

    ```
    # Minute    Hour     Day of Month    Month               Day of Week

    # (0-59)    (0-23)   (1-31)          (1-12 or Jan-Dec)   (0-6 or Sun-Sat)
    ```

11. Save and exit the vi session. Press **<ESC>** and type: **:wq**
12. Configure the permissions of the ntpd file to ensure proper operation:

    ```
    chmod 644 /etc/cron.d/ntpd
    ```

13. Once again, verify the current date and time:

    ```
    date
    ```

    The current time should be 10 minutes behind the correct time.

14. Update the system clock now by querying the NTP server with the NTP daemon:

    ```
    /usr/sbin/ntpd -q -u ntp:ntp
    ```

    The system responds with a message similar to the following:

    ```
    ntpd: time set +570.677029s
    ```

15. Finally, use the `date` command to verify that the time has been updated.

Creating the File Cache on the RAID

If your configuration does not include a RAID 5, continue to one of the following (as appropriate for your installation):

- Configuring MCS for MediaCentral UX and Media Composer Cloud
- Configuring MCS for Interplay MAM

In an earlier step you might have created a RAID 5 for the cache using the “arrays” utility built-in to the server’s BIOS. In this step you will partition the RAID, create a logical volume for the RAID and mount the MCS cache on it.

Partitioning the RAID

In this procedure you partition the RAID and write the new partition table entry to disk using the GNU parted disk partitioning utility.

The enclosure contains two devices of interest, the system disk (**/dev/sda**) and the RAID (**/dev/sdb**). Partitioning the system disk was performed automatically by the RHEL installer. You only need to partition the RAID, as indicated in this section.

Starting with RHEL 6.3, Red Hat creates a GPT volume when the MCS installation scripts initialize the cache volume during OS installation. GPT volumes must be handled using the GNU parted utility (rather than the Linux fdisk utility).

To partition the RAID:

1. Use the GNU parted utility to ensure the RAID 5 HD device exists:

    ```
    parted -l
    ```

Note that the command take a lower-case “L” (not a numerical “one”).

Information regarding the systems drives and partitions is displayed. If you have a RAID 5 array, it should be presented as “sdb” as in the example below:

```
Model: HP LOGICAL VOLUME (scsi)
Disk /dev/sdb: 2500GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End     Size    File system  Name  Flags
```

Take note of the Partition Table type. It will be listed as either “`msdos`” or “`gpt`”.

2. If the Partition Table for your RAID volume (sdb) is configured for “msdos”, you will need to convert it to “gpt”. If sdb is already formatted for “gpt”, you can skip this step.

   a. Enter the *parted* utility, specifying the volume you wish to work with (sdb):

   ```
   parted /dev/sdb
   ```

   The parted welcome screen appears and your user prompt changes from `#` to (`parted`).

   b. Convert the volume to use a “gpt” partition table:

   ```
   mklabel gpt
   ```

   c. You are asked to confirm that you wish to change the existing disk label:

   ```
   Warning: The existing disk label on /dev/sdb will be destroyed and all
   data on this disk will be lost. Do you want to continue? Yes/No?
   ```

   Type: **`Yes`**

   d. You are returned to the (`parted`) prompt. Type **`quit`** to exit the utility.

   A final message indicates that the `/etc/fstab` file might need to be updated. No action is required by you at this time.

3. Find the free space on the /dev/sdb device:

   ```
   parted /dev/sdb p free
   ```

   Information similar to the following is displayed:

   ```
   Model: HP LOGICAL VOLUME (scsi)
   Disk /dev/sdb: 2500GB
   Sector size (logical/physical): 512B/512B
   Partition Table: gpt

   Number  Start   End     Size    File system  Name  Flags
           17.4kB  2500GB  2500GB  Free Space
   ```

4. Create a primary partition on the RAID 5 using all the available space (2500 GB in the sample output provided above):

   ```
   parted -a optimal /dev/sdb mkpart primary ext2 0% 2500GB
   ```

   The system might respond with the following message:

   ```
   Information: You may need to update /etc/fstab
   ```

   The message can be ignored. You will update fstab when you create the logical volume and mount the cache for the new partition.

5. Set sdb partition “1” to type “logical volume”, and its state to “on”:

   ```
   parted /dev/sdb set 1 lvm on
   ```

6. Run the parted utility again to list your changes:

   ```
   parted -l
   ```

   ```
   Model: HP LOGICAL VOLUME (scsi)
   Disk /dev/sdb: 2500GB
   Sector size (logical/physical): 512B/512B
   Partition Table: gpt

   Number  Start   End     Size    File system  Name     Flags
    1      17.4kB  2500GB  2500GB               primary  lvm
   ```

   Notice in the above output the partition now has a partition number, is the primary partition, and has a logical volume flag. You create the file system in the next step.

If a non-writeable partition is detected, such as a disc located in an optical drive, the following message will appear:

```
Warning: Unable to open /dev/sr0 read-write (Read-only file system).
/dev/sr0 has been opened read-only.

Error: Invalid partition table - recursive partition on /dev/sr0.

Ignore/Cancel?
```

Investigate the warning if warranted and type "I" to continue.

Creating the Logical Volume, Filesystem and Mounting the Cache

In this procedure you work with the newly partitioned RAID 5 using the Linux Logical Volume Manager (LVM). The hierarchy of volumes in Linux is as follows: physical volume, volume group and logical volume.

To create the logical volume and mount the cache:

1. Create the physical volume:

   ```
   pvcreate --metadatasize=64k /dev/sdb1
   ```

   Note the name of the physical volume (/dev/sdb1) takes a 1 (one).

   LVM feedback indicates the successful creation of the physical volume.

2. Create a volume group, vg_ics_cache, containing the physical volume /dev/sdb1:

   ```
   vgcreate -s 256k -M 2 vg_ics_cache /dev/sdb1
   ```

   LVM feedback indicates the successful creation of the volume group.

3. Before creating the logical volume, obtain a value for the volume group's physical extents:

   ```
   vgdisplay  vg_ics_cache
   ```

   A list of properties for the volume groups appear, including the physical extents (Free PE). Physical extents are the chunks of disk space that make up a logical volume.

   Sample output is shown below:

   ```
   --- Volume group ---
     VG Name               vg_ics_cache
     System ID
     Format                lvm2
     Metadata Areas        1
     Metadata Sequence No  2
     VG Access             read/write
     VG Status             resizable
     MAX LV                0
     Cur LV                1
     Open LV               1
     Max PV                0
     Cur PV                1
     Act PV                1
     VG Size               1.09 TiB
     PE Size               256.00 KiB
     Total PE              4578332
     Alloc PE / Size       0 / 0
     Free  PE / Size       4578332 / 1.09 TiB
     VG UUID               cyWpGZ-s3PG-8UqH-4TBl-rvBA-33oJ-3uZt0u
   ```

Use the “Free PE” value to create a logical volume occupying the entire volume group (below).

4. Create the logical volume, lv_ics_cache, containing the volume group vg_ics_cache:

   ```
   lvcreate -l <Free_PEs> -r 1024 -n lv_ics_cache vg_ics_cache
   ```

   In the above command, replace *`<Free_PEs>`* with the value obtained in the previous step. This is the number before the slash in the “Free PE” line. No unit is needed.

   For example:

   ```
   lvcreate -l 4578332 -r 1024 -n lv_ics_cache vg_ics_cache
   ```

   Note the first switch in `lvcreate` is lower case “L”.

   LVM feedback indicates the successful creation of the logical volume. Note that Linux may override the sector size you specified. That is OK.

5. Create a filesystem on the logical volume (i.e. format it):

   ```
   mkfs.ext4 /dev/vg_ics_cache/lv_ics_cache
   ```

   In the above command, specify the logical volume by its Linux block device name (/dev/<volume_group>/<logical_volume>)

   As in other operating systems, formatting in RHEL is a slow operation. Please be patient.

   Feedback similar to the following indicates success:

   ```
   This filesystem will be automatically checked every 38 mounts or 180 days,
   whichever comes first. Use tune2fs -c or -i to override.
   ```

6. Edit the filesystem table:

   ```
   vi /etc/fstab
   ```

7. Add an entry at the end of the file:

   ```
   /dev/mapper/vg_ics_cache-lv_ics_cache /cache ext4 rw 0 0
   ```

   This automates the mapping of the logical volume to a file system directory (/cache in this case).

8. Save and exit the vi session. Press **<ESC>** and type: **`:wq`**

9. Mount the volume:

   ```
   mount /dev/mapper/vg_ics_cache-lv_ics_cache /cache
   ```

   Alternately, since you added an entry to fstab, you ought to be able to mount the cache as follows:

   ```
   mount /cache
   ```

If you receive an error indicating the mount point /cache does not exist, create the cache manually (`mkdir /cache`*) and issue the mount command again.*

10. Verify that /cache has been mounted correctly:

    ```
    df -h
    ```

    The following information is displayed about the cache: size, used, available, user % and mount point (mounted on), similar to the following:

    ```
    Filesystem                            Size  Used Avail Use% Mounted on
    /dev/mapper/vg_ics_cache-lv_ics_cache  29G  585M   27G   3%     /cache
    ```

11. Verify that /cache has the correct ownership and read-write-exec settings:

    ```
    ls -la /cache
    ```

    Information is displayed about the cache ownership, similar to the following:

    ```
    drwxr-xr-x   5 maxmin maxmin 4096 Oct 16 10:02 .
    ```

12. If the ownership is of /cache is not set to user maxmin, change its ownership:

    ```
    chown  maxmin:maxmin /cache
    ```

13. If the /cache directory does not have its read-write-exec settings are not *rwx* for *owner*, *group*, *other*, change the permissions:

    ```
    chmod  0777 /cache
    ```

14. Create the following two cache directories:

    ```
    mkdir /cache/download
    ```

    ```
    mkdir /cache/fl_cache
    ```

15. Change their ownership to user *maxmin*:

    ```
    chown maxmin:maxmin /cache/download
    ```

    ```
    chown maxmin:maxmin /cache/fl_cache
    ```

16. Change their permissions:

    ```
    chmod -R 02777 /cache/download
    ```

    ```
    chmod -R 02777 /cache/fl_cache
    ```

17. Verify that /cache and its subdirectories now have the correct ownership, read-write-exec settings, and *setgid* special permission:

    ```
    ls -la /cache
    ```

    Updated information is displayed, which ought to be similar to the following:

    ```
    drwxrwxrwx  5 maxmin maxmin 4096 Mar 22 10:04 .
    ```

User maxmin owns the MCS process that writes to the cache. Avid processes will create subdirectories in /cache, on an as-needed basis.

Enabling / Disabling 3G and Edge Streams

By default, MCS servers encode assets in three different media streams (Wi-Fi, 3G, and Edge) for playback on mobile devices. If your facility intends to connect mobile devices through Wi-Fi only, it is recommended that you disable the 3G and Edge streams, to improve the encoding capacity of the MCS server. If your facility does not intend to connect any mobile devices to the MediaCentral system, this file does not require editing. Mobile media formats are only created if a device running the MediaCentral UX Mobile application connects and attempts to play media.

To Disable 3G and or Edge Streams:

1. Use the Linux *vi* editor to edit the following file:

    ```
    vi /usr/maxt/maxedit/share/MPEGPresets/MPEG2TS.mpegpreset
    ```

2. In each of the [Edge] and [3G] areas, set the active parameter to **`active=0`**.

3. Save and exit the vi session. Press **<ESC>** and type: **:wq**

To re-enable 3G or Edge, edit the file and reset the "active" value to 1.

Upgrading the Avid Shared Storage Client Software

MediaCentral Platform Services includes a copy of both the Avid ISIS Client and the Avid NEXIS Client software. The ISIS Client is installed by default through the MCS installation process. The NEXIS Client is bundled with the MCS software for convenience, but is not actively installed. Verify the version of the Avid NEXIS or Avid ISIS client required for your environment and upgrade the client software if necessary.

For version compatibility information, see the "Compatibility Matrix: Interplay Production and MediaCentral" on the Avid Knowledge Base.

To upgrade the shared storage client:

1. Prior to upgrading the shared storage client, you must first stop the ICPS back-end services that use the storage client:
   - For a single server, use the following command:

     ```
     service avid-all stop
     ```

   - If you are referring to this process to upgrade the shared storage client on an established MCS cluster configuration, issue the following command from any node to stop the cluster resource that manages the service:

     ```
     crm resource stop AvidAllEverywhere
     ```

2. Navigate to the location of the bundled shared storage client software:

   ```
   cd /opt/avid/Packages
   ```

3. Use the following command to upgrade the shared storage client:

   ```
   rpm -Uvh AvidNEXISClient-<version>.el6.x86_64.rpm
   ```

   You do not need to uninstall any previous version of the client software. The installer automatically replaces the version of the client already installed on the system.

   If you are referring to this process to upgrade the shared storage client on an established MCS cluster configuration, repeat this step on all cluster nodes.

4. Once the client is installed, restart the avid-all service:
   - For a single server, use the following command:

     ```
     service avid-all start
     ```

   - If you are referring to this process to upgrade the shared storage client on an established MCS cluster configuration, issue the following command from any node to stop the cluster resource that manages the service:

     ```
     crm resource start AvidAllEverywhere
     ```

Upgrading the client on a cluster might introduce resource fail-counts. Use the Cluster Resource Monitor, `crm_mon`*, to verify the status of the cluster and if necessary, clear the fail-counts with the* `crm resource cleanup <rsc> [<node>]` *command.*

5. Verify the version number of the updated client software:

   ```
   rpm -qa | egrep -i 'isis|nexis'
   ```

   This command returns all installed packages with either ISIS or NEXIS in the name.

If for any reason you need to revert to the original ISIS client, see "Downgrading the Avid Shared Storage Client" on page 263 for complete instructions.

Copying Software to the MCS Server

Now that the basic RHEL installation is complete, you might need to copy additional software to the MCS server. Common software includes:

- RHEL Security Patches
- MCS Software Updates
- Additional packages such as the Closed Captioning Service or the MAM Connector

For more information, see "Copying Software to the MCS Server" on page 24.

Installing Security Updates

Once you have installed the operating system, consult the "Security Updates" section of the *Avid MediaCentral Platform Services ReadMe* to resolve any outstanding RHEL security vulnerabilities. While some security updates are recommended, others are **required** to be installed on the MCS servers.

Once the security patches have been installed, users can run the `avid-security-check` script to verify the installation. To run the script, type the following command:

```
avid-security-check
```

Review the output and resolve any updates that are listed as FAILED, as shown in the following example:

```
Check security update for: openssl
        required version:  openssl-1.0.1e-30.el6_6.5
        installed version: openssl-1.0.1e-30.el6_6.5       [  OK  ]

Check security update for: glibc
        required version:  glibc-2.12-1.166.el6
        installed version: glibc-2.12-1.132.el6            [FAILED]
```

Installing Software Patches

Avid releases patches for MCS on a regular basis to assist in addressing customer issues and feature requests. Refer to the *Avid MediaCentral Platform Services ReadMe* for information on current patches and install any available patches at this time.

4 Configuring MediaCentral

Chapter Overview

Now that you have installed and configured the operating system, you are ready to configure the software and settings specific to MediaCentral.

⚠ **If you are running a cluster, complete the steps in this chapter on the master node only (unless instructed otherwise). Settings will be replicated to the other nodes during the cluster configuration process.**

This chapter is divided into two main sections. Proceed to the section appropriate for your installation:

- Updating the MediaCentral UX Configuration

  This section includes information on multiple workflows such as iNEWS, Interplay Production, Media Composer Could, Send To Playback, etc. Read and apply the sections appropriate for your installation.

- Configuring MCS for Interplay MAM

  This section includes the steps required to configure MediaCentral Platform Services for integration with Interplay MAM.

The following table lists the topics that cover the configuration of MCS for MediaCentral UX and Media Composer Cloud:

Step	Task	Time Est.
1	Updating the MediaCentral UX Configuration	2 min
	Covers use of the Configurator Tool.	
2	Signing into MediaCentral UX	5 min
	This section details the process for signing in to MediaCentral UX for the first time.	
3	Changing the Administrator Password	2 min
	For security it is recommended you change the administrator password.	
4	Creating a Second Administrator User	5 min
	Helps to ensure you do not get locked out of the interface.	
5	Configuring System Settings	varies
	Covers the configuration of the MediaCentral System Settings.	
6	Enabling Asset Watermarking	varies
	Optionally add a custom watermark to the player for asset protection.	

Step	Task	Time Est.
7	Verifying the System Settings	varies
	A process for testing the configured settings.	
8	Configuring Send To Playback Settings	5 min
	Configure settings for STP workflows.	
9	Importing Domain Users	5 min
	Covers the process of importing Windows Domain Users.	
10	Creating Local Users and Assigning Roles	varies
	Information on creating local users and role assignments.	
11	Continuing the Installation	1 min
	Suggestions for additional steps to continue your installation.	

The following table lists the topics that cover the configuration of MCS for Interplay MAM:

Step	Task	Time Est.
1	Configuring MCS for Interplay MAM	5 min
	Introduction to MCS for MAM and prerequisites.	
2	Mounting MAM Storage	5 min
	Information related to the process for mounting MAM storage volumes.	
3	Configuring the ACS Gateway Access Port	5 min
	Verify the setting on the MAM server that enables access to the avid-acs-gateway.	
3	Configuring the MediaCentral User Interface	5 min
	Verify the enabled components of the configurator.	
4	Creating the MAM System User	5 min
	Create the specialized user to be used with MediaCentral.	
5	Configuring the MCS Player	5 min
	Updating the Player Site Setting within MediaCentral UX.	
6	Enabling Remote Playback	10 min
	Description and process for enabling the alternate Remote Playback workflow.	
7	Continuing the Installation	1 min
	Suggestions for additional steps to continue your installation.	

Updating the MediaCentral UX Configuration

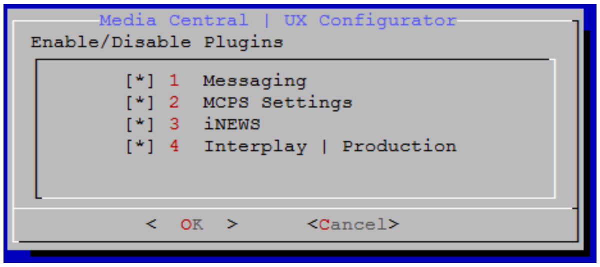
By default, MediaCentral enables functionality for MCPS Settings, iNEWS and Interplay | Production workflows. Additional features such as Media Distribute can be added to the system through the MediaCentral UX Configurator Tool. Features that are not required for your installation should be disabled. If you are configuring a cluster, this step only needs to be completed on the master and slave nodes. However, it is good practice to run the configurator on all nodes. At this point in the installation, this step can be completed on all nodes concurrently.

To verify or alter MediaCentral functionality:

1. Start the configurator by typing the following at the Linux prompt:

   `/opt/avid/avid-interplay-central/configurator`

   The configuration UI appears.



```
Media Central | UX Configurator
Enable/Disable Plugins

        [*] 1  Messaging
        [*] 2  MCPS Settings
        [*] 3  iNEWS
        [*] 4  Interplay | Production

          <  OK  >       <Cancel>
```

Additional plug-ins such as Media | Distribute appear in the Configurator only if the features have been installed on the system (through a separate install process).

2. Select the appropriate application profile settings.

   The following table outlines typical settings by deployment type:

	Messaging	MCPS Settings	iNEWS	Interplay Production
MediaCentral (default settings)	(optional)	ON	ON	ON
Interplay Production Only	(optional)	ON	OFF	ON
iNEWS Only	(optional)	OFF	ON	OFF
Media Composer Cloud	(optional)	ON	OFF	ON
Interplay MAM	(optional)	ON	OFF	OFF

- **Messaging**: Enables or disables the Messages pane for all layouts.
- **MCPS Settings**: Toggles the MCPS group in the System Settings layout. This group provides access to the Load Balancer, Playback Services and Player settings details pages.
- **iNEWS**: Toggles the iNEWS settings group.
- **Interplay Production**: Toggles the Interplay Production settings group.

For example, administrators creating an iNEWS-only deployment without video playback would enable iNEWS and disable MCPS Settings and Interplay Production. Messaging is optional.

3. Use the Up and Down arrow keys to move between the options, Left and Right arrow keys to move between OK and Cancel, SPACEBAR to toggle the asterisks, and press Enter to confirm.

   - Asterisk = enabled
   - No Asterisk = disabled

   Now when you access MediaCentral UX, the UI will be correctly configured for your deployment.

For more information, see "Working with the MediaCentral UX Configurator" on page 259.

Signing into MediaCentral UX

MCS servers are configured using the MediaCentral UX System Settings. This process is completed through the use of a web browser such as Google Chrome.

If you are configuring a cluster, you configure the MediaCentral UX System Settings once on the master node only. Do not configure these settings on slave or load balancing nodes. The other nodes inherit settings from the master through the clustering mechanisms. ***Complete all remaining sections of this chapter on the Master node only****.*

To sign into MediaCentral UX:

1. Launch a supported web browser or use the MediaCentral UX Desktop application to access MediaCentral UX.

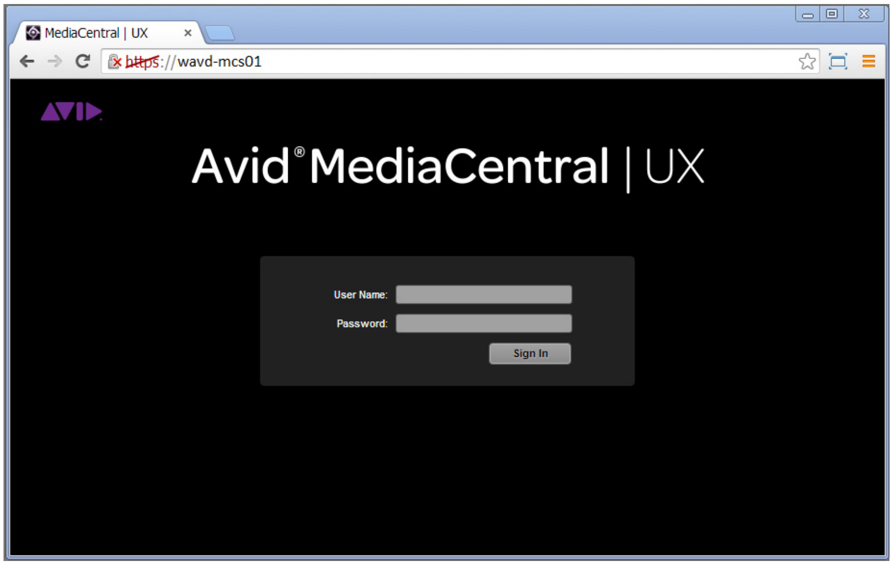
   Supported browsers include: Google Chrome or Safari (on Mac OS).

2. Enter the URL of the MCS server in the address bar:

   `https://<hostname>`

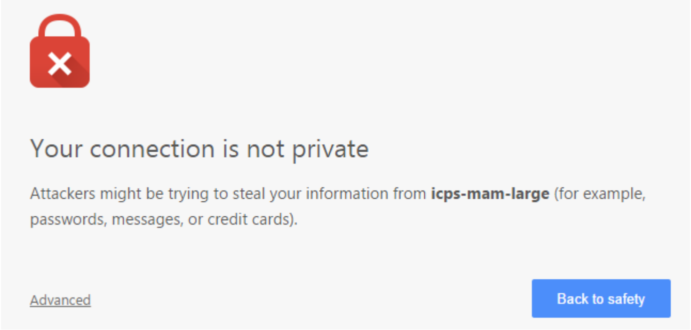
   Where <*hostname*> is the Fully Qualified Domain Name (FQDN) of the MCS server.

   The MediaCentral UX sign-in screen appears.



In place of the sign-in screen, you might see a warning indicating the connection is not private. The warning relates to SSL certificates.

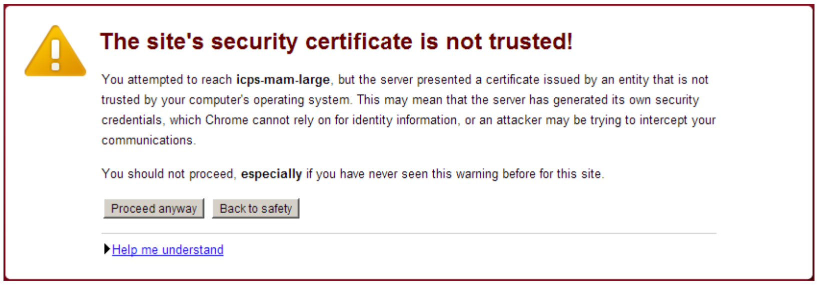
For the purposes of installing and configuring MediaCentral UX, ignore the warning by clicking the Advanced link and then clicking the Proceed to <MediaCentral URL> (unsafe) link.



Your connection is not private

Attackers might be trying to steal your information from **icps-mam-large** (for example, passwords, messages, or credit cards).

In older versions of Chrome (previous to release 37), the following warning is shown instead:



The site's security certificate is not trusted!

You attempted to reach **icps-mam-large**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

In the above case, click the Proceed Anyway button.

For information on configuring a trusted certificate, see the following article on the Avid Knowledge Base: http://avid.force.com/pkb/articles/en_US/how_to/SSL-Certificates-for-server-to-browser-connections.

3. Enter the Administrator user and password to access MediaCentral UX:

   - User name: Administrator
   - Default Password: Avid123

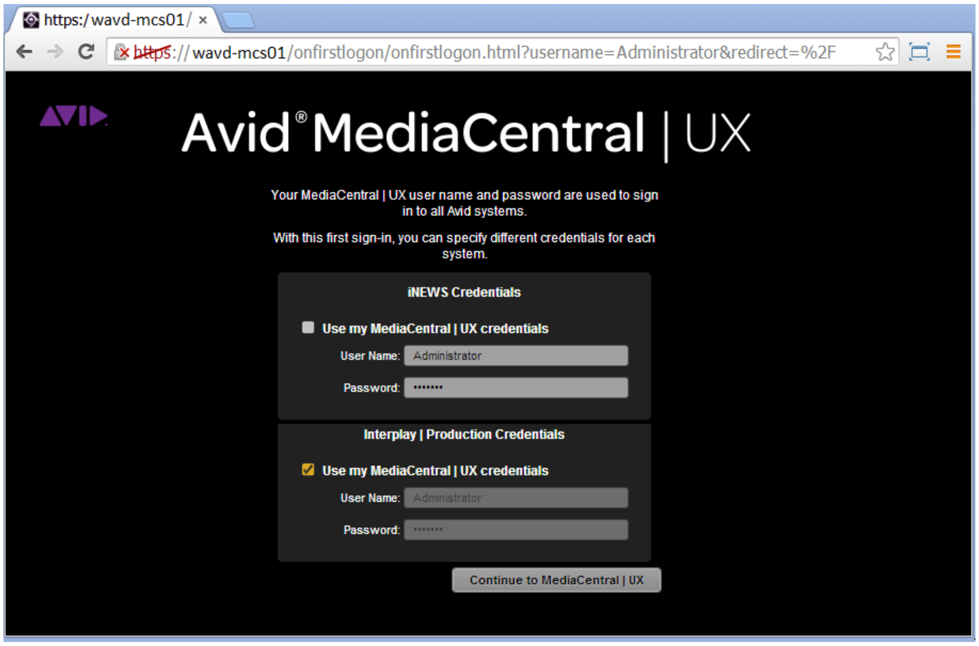
4. The first time any user signs in, the Avid Software License Agreement is presented.

   Click the Accept License Agreement button to proceed.

5. Enter your account information. When you sign in to MediaCentral for the first time you are prompted to enter your user credentials for iNEWS, Interplay Production, or both. Sign in options depend on the features selected in the MediaCentral UX Configurator.

   If you created custom iNEWS and Interplay Production credentials (e.g. MCSAdmin), enter that information at this time. Otherwise, leave the defaults (Administrator / Avid123).

If the security settings for one of these systems is inaccurate, you will see a warning message that states that the application is unable to authorize the sign-in name or password. This will be the case for any iNEWS credentials entered, since you have not yet specified the iNEWS server to be used. If you receive a warning, click the link provided and verify your security settings.



https:/wavd-mcs01/ ×
~~https~~://wavd-mcs01/onfirstlogon/onfirstlogon.html?username=Administrator&redirect=%2F

Avid® MediaCentral | UX

Your MediaCentral | UX user name and password are used to sign in to all Avid systems.

With this first sign-in, you can specify different credentials for each system.

iNEWS Credentials

□ Use my MediaCentral | UX credentials

User Name: Administrator

Password: •••••••

Interplay | Production Credentials

☑ Use my MediaCentral | UX credentials

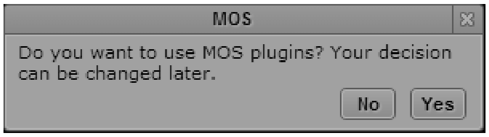
User Name: Administrator

Password: •••••••

6. Click the “Continue to MediaCentral UX” button.
7. If you are accessing MediaCentral UX through Chrome or Safari, you might be asked if you want to “Send notifications”. This is related to the Desktop Notifications feature introduced in MCS v2.4. Select either the Allow or Block option when presented with this message.

   If desired, this feature can be disabled. For detailed instructions, see “Modifying application.properties” on page 252.

   For more information on the Desktop Notifications feature, see the *Avid MediaCentral | UX User’s Guide.*
8. If you are accessing MediaCentral UX through Chrome v44 or earlier and you enabled iNEWS in the MediaCentral Configurator tool, the first time you sign in to MediaCentral a dialog box asks if you want to use MOS plug-ins:



MOS

Do you want to use MOS plugins? Your decision can be changed later.

Selecting “Yes” enables the “MOS enabled” check box in the user settings and prompt you to install the container needed for Active X controls.

Selecting “No” does not enable the MOS check box or prompt you to install any additional software. The MOS check box can be enabled manually in the user’s settings at any time.

MOS plug-ins require additional software as described in “Avid MediaCentral | UX Desktop” on page 302.

Active X controls and MOS plug-ins are not supported in the Safari browser or in Chrome v45 or later. If you are running MCS v2.7 or later with Chrome v45 or later, you will not receive this dialog box. If you are running Chrome v44 or earlier, MOS options are still available.

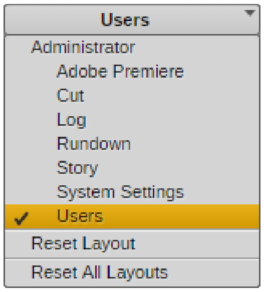
If you are using Chrome and require continued use of MOS plug-ins, see "Avid MediaCentral | UX Mobile Application" on page 296 for an alternative method of connecting to MediaCentral UX.

Changing the Administrator Password

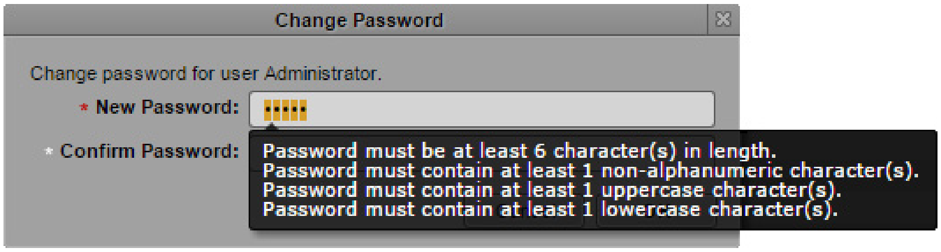
For security reasons, it is strongly suggested that you change the password for the Administrator user account.

To change the Administrator password:

1. While logged in as the Administrator, select Users from the Layout selector.



2. Expand the list of Administrators in the User Tree and locate the Administrator user.
3. Double-click on the Administrator account. Details will appear on the right.
4. Click the Change Password button in the Details pane, and enter a new password for the Administrator user.



Change password for user Administrator.

* New Password: •••••

* Confirm Password:

Password must be at least 6 character(s) in length.
Password must contain at least 1 non-alphanumeric character(s).
Password must contain at least 1 uppercase character(s).
Password must contain at least 1 lowercase character(s).

MediaCentral v2.1 introduced strong password enforcement. This feature was made optional in v2.2; however the default is to have strong passwords enabled. For more information on this feature and a process for "Turning Off Secure Password Requirements", see the Avid MediaCentral | UX Administration Guide.

5. Click OK update the password information.

   A message appears indicating that the password was successfully changed.

Creating a Second Administrator User

In the event that you are locked out of MediaCentral for any reason, it is wise to create a second Administrator-level user.

To create a backup administrator acount:

1. While in the Users Layout, highlight the Administrators group in the User Tree.
2. Click the Create User button under the User Tree tab.
3. In the Details pane, assign a User Name.
4. Enter a Password and confirm the password.
5. Deselect the check box for “User must change password at next sign-in.”
6. Click the Save button in the bottom-right corner of the window.

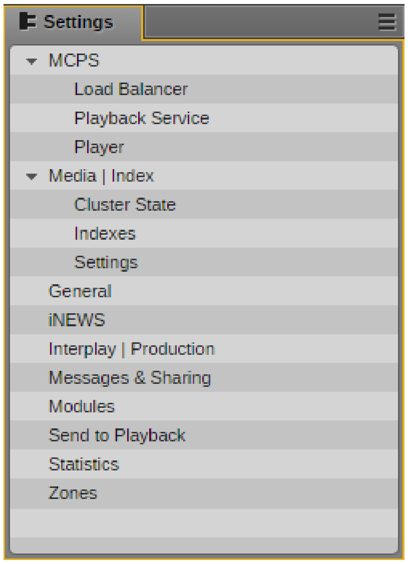
   The user account is created.

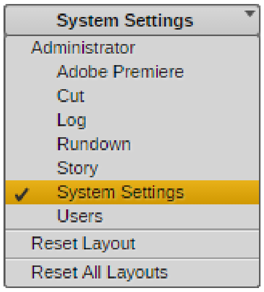
Configuring System Settings

Much of the configuration of MediaCentral is completed through the System Settings. Proceed through the following sections and configure settings applicable to your configuration. For more information, see the *Avid MediaCentral | UX Administration Guide*.

If you are configuring a cluster, you configure the MediaCentral UX System Settings once on the master node only. Do not configure these settings on slave or load balancing nodes. The other nodes inherit settings from the master through the clustering mechanisms.

To access the System Settings, select “System Settings” from the Layout selector in the top-right corner of the interface. This layout will only appear if you are logged in as a user with Administrator rights.





This image shows the default list of System Settings. As features are added to the system, the list might include additional line items such as Media Distribute, Customizable Logger, and others.

General Settings

This section configures general settings related to the overall operation of MediaCentral UX.

Although “General” is not the first item in the list of settings, configure the settings as outlined in this document, starting with the General category.

To configure the General settings:

1. In the Settings pane, select **General**.
2. System ID: Every MCS system can be identified with a System ID provided by Avid at point of sale. This ID can be used to access Avid Customer Care for systems with valid support contracts.

   Once entered, the ID is stored with the ACS bus configuration information. The System ID is displayed when you invoke the `ics_version` command from Linux or when you select Home > About within the MediaCentral UX user interface.

If you cannot locate your System ID, contact your Avid representative.

3. Search Pane: Specify the maximum number of assets to be displayed in a search. The default value of this field is 50.
4. Session Timeout: Specify the number of minutes of inactivity before the user’s session is disconnected. The range of this value is between 10 minutes and 1440 minutes (24 hours). The default value of this field is 30 minutes. As of MediaCentral v2.1.0, this feature can be enabled or disabled.
5. Time Zone: Use the pull-down menu to select a default time zone for the local MediaCentral system. This information is used to properly display assets when doing searches outside of the local system. Examples:
   - US/Eastern
   - Europe/London
   - Asia/Hong_Kong
6. Date Format: Use the pull-down menu to select a default date format for the local MediaCentral system. This information is used to properly display assets when doing searches outside of the local system. Options:
   - DD.MM.YYYY hh:mm:ss
   - DD/MM/YYYY hh:mm:ss
   - YYYY-MM-DD hh:mm:ss
   - MM/DD/YYYY hh:mm:ss
7. Click Apply to save your changes.

iNEWS Settings

This section configures settings related to Avid iNEWS. ICS v1.0 – v1.4 supported connection to only one iNEWS system. iNEWS Community support was added in ICS v1.5 with up to 24 members. iNEWS V3.7 and iNEWS V4.7 expanded support to 50 community members which is supported with ICS v1.8 and later.

To configure the iNEWS settings:

1. In the Settings pane, select **iNEWS**.
2. System ID: Enter the System ID for your iNEWS system.

   This information can be found on the iNEWS server(s) in the `/site/system` file. If your iNEWS system consists of multiple servers for load balancing and fail-over, using the System ID ensures that MediaCentral connects to iNEWS properly.

   iNEWS servers will often include a "–a" or "–b" suffix in their hostname. Do not include these suffixes when entering the System ID information. Ensure that all MediaCentral servers can resolve the hostnames and IP addresses of all iNEWS servers through DNS.
3. Timing: This value specifies how the iNEWS timing field is updated when you associate a sequence with a story.
4. Tape ID: When you associate a sequence with a story, this iNEWS field name is associated with the sequence's Tape-ID field

   Example iNEWS field: video-id
5. Pagination: The maximum number of items listed in the Queue/Story pane or the Project/Story pane. To view more items beyond the number displayed, click the Show More Results button. The range is 5 to 255 items. The default value of this field is 50.
6. Click Apply to save your changes.

Interplay Production Settings

This section configures settings related to Interplay Production. Avid supports connecting MediaCentral to only one Interplay Production system per MCS installation.

To configure the Interplay Production settings:

1. In the Settings pane, select **Interplay | Production**.
2. Interplay | Production Server: Enter the (short) hostname or virtual hostname of the Interplay Production Engine. An IP address is also acceptable here. Do not use a Fully Qualified Domain Name (FQDN) in this field.
3. MCDS Service URL: Enter the URL of the server or servers hosting the MediaCentral Distribution Service. You can enter a hostname or IP address for the server. The standard port number used by this service is 8443. If you have installed multiple copies of MCDS, list each URL separated by a comma and a space. Multiple instances of MCDS provide fail-over capability, but not load balancing.

   Example: https://wavd-tc01:8443
4. Location for Script Sequence:

   a. In the Path field, specify a folder in the Interplay Production database where script sequences will be stored. The correct path format does not include a leading slash.

      Example: Projects/iNEWS or iNEWS/Scripts

   b. Select whether you want sub-folders in the parent folder to be created by Queue name, Date, or Story name.
5. Assets Pane: Sets the max number of Interplay assets to display at one time. This value can range between 5 and 1000. The default value for this field is 50.
6. Click Apply to save your changes.

Messages & Sharing

These settings enable messages delivered through the messaging service to be forwarded to user's individual email accounts. These settings have nothing to do with emails sent from the MCS cluster or other Linux processes. Only messages created in the Messaging pane are forwarded.

To configure the Messages & Sharing settings:

1. In the Settings pane, select **Messages & Sharing**.
2. Message Archiving: Configure the number of days to retain active messages. Messages older than this will be archived. The default value of this field is 7.

For instructions on retrieving archived messages, see the Avid MediaCentral | UX Administration Guide.

3. Email Forwarding: If email forwarding is desired, enable the check box for this option. Consult with your in-house IT Department for this information.
   a. SMTP server hostname: Enter an SMTP server hostname.

      Example: webmail.wavd.com

   b. Port: Enter a communication port. The default port is 25.
   c. User name: Enter a username in the form of an e-mail address.

      Example: admin@wavd.com

   d. Password: Enter the password for the associated user account.
   e. Use SSL (Secure Sockets Layer): Select this check box if required by IT.
   f. Ignore TLS (Transport Layer Security): Select this check box if required by IT.
4. Email Options: This feature allows the Administrator to customize the content of messages forwarded to the user's e-mail.
   a. If a user sends a message with a media asset, enabling the "Don't include asset" check box eliminates the inclusion of a link to that asset. This is useful if the site's default web browser is not supported by MediaCentral UX (such as Internet Explorer).
   b. If desired, enter a customized message header.
   c. If desired, enter a customized message footer.
5. Once you have configured the email forwarding fields, verify functionality by entering a recipient email and clicking Validate.

If the e-mail is not received, verify with your IT Department that ICMP traffic is allowed through appropriate firewalls and network switches.

6. Click Apply to save your changes.

Playback Service Settings

This section configures settings related to MediaCentral Playback Services (MCPS). MCPS is a set of services which run on the MCS servers that are responsible for the compression and playback of video and audio media.

To configure the Playback Service settings:

1. In the Settings pane, select **MCPS > Playback Service**.
2. Player Settings: The "Save Failed AAF" feature automatically saves AAF files that do not parse properly to a dedicated folder (`/cache/aaf_to_investigate`) on the MCS server. This feature can assist in troubleshooting efforts and should only be enabled upon request from Avid Customer Care.
3. Interplay Workgroup Properties:
   a. User / Password: MediaCentral requires a dedicated user to access the Interplay Production database. Enter that user and password.

      Suggested User Name: MCSAdmin

   b. Workgroup Name: Enter the name of the Interplay Production Workgroup (Framework). The Workgroup Name is case sensitive.

   c. Lookup Servers: Enter the (short) hostname of the server hosting the Interplay Production Framework Lookup Service. If there are multiple Lookup Servers, enter each hostname separated by a comma. Do not use a Fully Qualified Domain Name (FQDN) in this field.

   d. Enable Dynamic Relink: Enable this option if you are working in a multi-resolution environment. If enabled, the player links to the lowest resolution associated with the asset. If this option is disabled, the player links to the media associated with the asset at the most recent checkin. This option is also required for sending high-resolution media to a playback device (STP).

MCS v2.5 and later obtains the Media Indexer configuration information directly from the "Server Hostname Settings" in the Interplay Administrator tool. Settings found in previous releases regarding the Media Indexer HAG and MI Host have been removed from MCS v2.5.

4. General ISIS Settings:
   a. Enable Remote Host: If you are connected to Avid shared storage through a Zone1 or Zone2 network connection, leave this box unchecked. If you are connecting through Zone3 (preferred configuration type), enable this check box.

      For a refresher on zone definitions, see "Network Interface Cards and Network Connections" on page 19.

   b. Use Network Device: If you have multiple network interfaces configured and enabled on the MCS server, enter the name of the interface used to connect to Avid shared storage. Multiple interfaces can be entered, separated by a comma. This field can be left blank if the MCS server has only one active network connection.

      Examples: eth0 or em1

   c. Ignore Network Device: If you have multiple network interfaces configured and enabled on the MCS server, enter the name of the interface that will not be used to connect to Avid shared storage. Multiple interfaces can be entered, separated by a comma. This field can be left blank if the MCS server has only one active network connection.

      Examples: eth1 or em2

d. Connection Mode: Select the type of connection used to connect to Avid shared storage.

   Options: 1GB Connection or 10GB Connection

5. Storage Locations. This section provides settings enabling MCS to connect to Avid shared storage.

   a. Click the plus '+' button to add a Storage Location.

   b. A "New File System" box will appear. Give the Storage Location a nickname and click Ok.

      Examples: "WAVD ISIS 7500" or "Production NEXIS"

      The Type "ISIS" is applicable to both Avid ISIS and Avid NEXIS systems.

   c. Click OK. Additional fields will appear below the Storage Locations.

   d. Virtual Host Name: Enter the **virtual** hostname of the share storage system. Every NEXIS and ISIS system has a virtual hostname, regardless of it being a single or fail-over configuration. **The Virtual Host Name must be entered in all lower-case**.

   e. User / Password: MediaCentral requires a dedicated user to access the storage system. Enter that user and password.

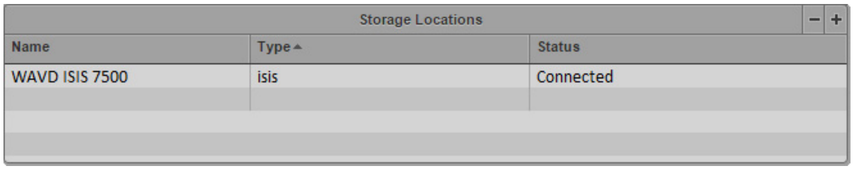
      Suggested User Name: MCSAdmin

      If you are connecting to multiple shared storage systems, ensure the same user/password is created on each system.

   f. System Directors: If you are connecting through Zone 3, enter the IP address(es) of the System Director(s). Do not add the virtual IP addresses. Each IP address should be separated by a semicolon (no spaces).

   g. Repeat these steps if configuring more than one Avid shared storage connection.

6. Click Apply to save your changes. As the settings apply, MediaCentral will attempt to connect to the system(s) you have specified.



Name	Type▲	Status
WAVD ISIS 7500	isis	Connected

If the connection is made successfully, the Status field should change from "Disconnected" to "Connected".

Player Settings

This section configures settings related to the MediaCentral Player. The MCPS Player communicates directly with the MCS server to obtain media for playback, using the credentials of the logged-in user for validation.

To configure the Player settings:

1. In the Settings pane, select **MCPS > Player**.
2. Server: Enter the Fully Qualified Domain Name (FQDN) of the MCS server. Entering a short hostname or IP address in this field can lead to playback issues.

   Example: wavd-mcs01.wavd.com

   If you are in the process of setting up the first server in a cluster, enter the FQDN of the server you are working on (node1 of the cluster). Later in the process, you will update this field with the virtual cluster hostname.
3. Media Composer | Cloud User: If your configuration consists of a Media Composer Cloud workflow, enter the user name and password for the Cloud user.

   Suggested User name: cloud

   If your workflow does not include Media Composer Cloud, these fields can be left blank.

   As a reminder, the Cloud User is a custom account that is added here and in the Interplay (Production) Administrator. This must be a unique user created solely for this purpose. This user should not be created as an Interplay Production or an Avid shared storage user.

If the credentials do not match, the Media Composer Cloud console will present a "Sphere XKAsset Error: 6" indicating an invalid username and password.

If you need to delete the Cloud user, you are advised to delete the user from the System Settings > Player layout, rather than in the Users pane.

4. Variable Speed Playback: If desired, adjust the values used when JKL shuttling.

   For more information on this feature, see the *MediaCentral UX Administration Guide*.
5. Image Quality Settings: If desired, the playback image quality can be adjusted to provide higher image quality to the user.

Adjusting the Image Quality Settings affects overall performance of the MediaCentral system. This could result in additional hardware requirements such as expanding from a single node server to a cluster or adding additional nodes to an existing cluster.

   This section also controls the ability for users to export MP4 files from the Media pane. This option is not enabled for all users by default to allow system administrators the ability to control who can export potentially sensitive data.

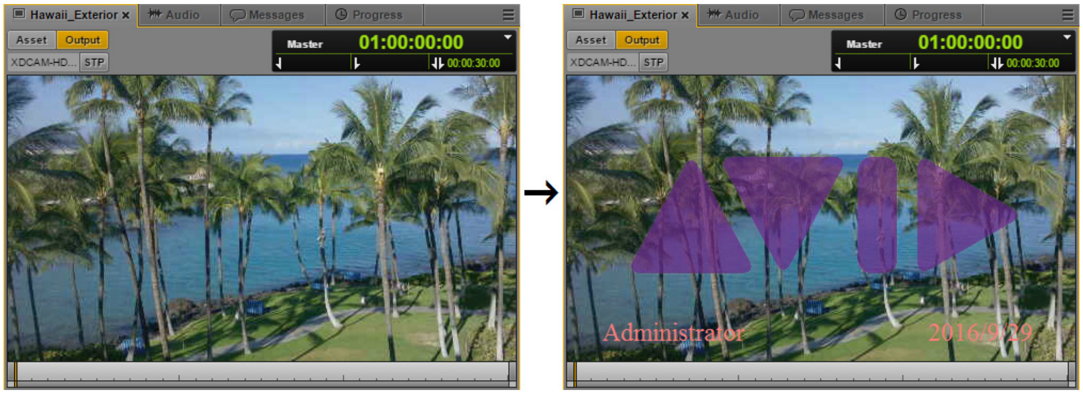
   For more information on these features, see the *MediaCentral UX Administration Guide*.

6. Click Apply to save your changes.

Enabling Asset Watermarking

MediaCentral Platform Services v2.9 includes a Technology Preview of the Asset Watermarking feature for use with all video assets. For sites that want to add a layer of protection from unauthorized or unlawful distribution of copyrighted media, an image can now be superimposed on top of any asset processed through the MediaCentral player service. In addition to the superimposed image, the current user name and date stamp are also added to the image.

The following is an example of the MediaCentral | UX Media pane, before and after watermarking has been enabled:



Watermarking affects any system that requests frames from the player service. This includes MediaCentral | UX, Media Composer | Cloud, Interplay | MAM, and the MediaCentral | UX mobile app. Exported assets such as MP4 files and PNG / JPEG graphics are also affected by the watermark.

Watermarks are not added to media that is processed through a Send To Playback request or through Media | Distribute as these assets are processed through other (non-player) systems.

This workflow is only supported with frame-based playback. For more information on frame and file-based playback, see “Selecting Frame-Based Playback or File-Based Playback” in the *Avid MediaCentral | UX User’s Guide*.

The overlay graphic must adhere to the following guidelines:

- File type: Targa (TGA)
- Image size: 1280 x 720
- Alpha channel: Required
- Resolution: 8 bits / channel (uncompressed)

Other file formats can introduce a negative impact on system performance. Unsupported file types result in a “Media Offline” message in the Media pane.

Some notes about the User and Date stamps:

- The font, point size, and text color cannot be altered at this time.
- The User and Date stamps are automatically displayed when you enable the Watermarking feature. If a valid image file is not added to the location specified in the path below, the User and Date stamps appear but the image does not.

Configuring Asset Watermarking

If your system will be configured in a cluster, you must complete the following process on all nodes, in any order. This is required because the MCS player services run on all cluster nodes.

To add watermarks to MediaCentral assets:

1. Create an overlay image file using the values specified above.
2. Create a new folder in the `/cache` directory to store the image. For example:

   ```
   mkdir /cache/watermark
   ```

3. Change the ownership of the watermark directory to the “maxmin” user. For example:

   ```
   chown maxmin:maxmin /cache/watermark
   ```

4. Copy the image file to the newly created directory.

   For detailed instructions, see “Copying Software to the MCS Server” in the *MediaCentral Platform Services Installation and Configuration Guide*.

5. Use the vi editor to open to the configuration file that contains information about the watermark variables:

   ```
   vi /etc/sysconfig/avid-common-params
   ```

6. Arrow-down to the location in the file that contains information on the watermark options and edit the line that contains the path and image file name:

   ```
   #export AVID_XMD_WATERMARK_IMAGE="/cache/watermark/image.tga"
   ```

   Make the following changes:

   - Remove the “#” symbol to uncomment the line.
   - Alter the path to the folder that you created to store the watermark image file.
   - Alter the name of the image file.
   - Add quotes around the image path and file name.

   For example, the altered line might look like the following:

   ```
   export AVID_XMD_WATERMARK_IMAGE="/cache/watermark/avid.tga"
   ```

   If desired, you can also remove the “#” symbol from the line that indicates the image opacity and alter the default value. The acceptable range for this value is 1 to 100.

The START_IMAGE and END_IMAGE values are for future use and must not be altered at this time.

This file is not replaced when upgrading from a previous version of MediaCentral Platform Services. If you do not see the values listed above, delete or rename `avid-common-params` *and restart the avid-all service to regenerate the file with the updated options.*

Adjusting the values in this file could have negative consequences on system performance. Only adjust the values in this file as directed in this guide.

7. Save and exit the vi session. Press <ESC> and type: **`:wq`**
8. Restart the avid-edit service to enable the configuration changes:

   ```
   service avid-edit restart
   ```

   This step temporarily disconnects users from the playback service. Playback is briefly interrupted, but users are not logged out of the system.

If you are configuring Asset Watermarking for a cluster that is already in operation, issue the following command once from any cluster node to restart the cluster resource that manages the avid-edit service: `crm resource restart AvidAllEverywhere`

9. If you are configuring multiple nodes for a cluster configuration, repeat the above steps on all nodes.

Updating the Watermark Image

The overlay image can be changed at any time by simply replacing the graphic file located on the MediaCentral servers and restarting the avid-edit service.

To update the watermark image:

1. Copy the updated watermark image to the `/cache/watermark/` directory using the copy method of your choice.
2. Restart the avid-edit service on the MediaCentral server(s).
   - For single-server installations:

     ```
     service avid-edit restart
     ```
   - For systems already running in a cluster configuration:

     ```
     crm resource restart AvidAllEverywhere
     ```

Disabling Asset Watermarking

The feature can be easily disabled by either deleting or commenting-out the configuration information in the `avid-common-params` file.

To disable Asset Watermarking:

1. Open the “avid-common-params” file for editing using the Linux vi editor:

   ```
   vi /etc/sysconfig/avid-common-params
   ```
2. Find the location of the text added to the file when the feature was first enabled:

   ```
   export AVID_XMD_WATERMARK_IMAGE="/cache/watermark/<image.tga>"
   ```
3. Either delete this line or add a pound symbol (#) in front of the text:

   ```
   #export AVID_XMD_WATERMARK_IMAGE="/cache/watermark/<image.tga>"
   ```
4. Save and exit the vi session. Press <ESC> and type: **`:wq`**

Verifying the System Settings

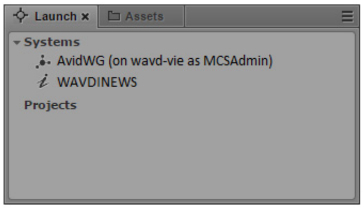
Now that you have configured the base system settings for connecting to iNEWS, Interplay Production and Avid shared storage (as applicable); perform some initial testing. If you are currently signed in to MediaCentral UX, sign out of MediaCentral UX and sign back in again prior to testing. This ensures the user has access to the updated System Settings.

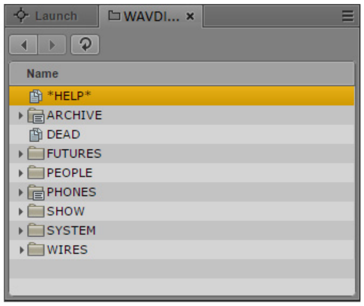
Verifying the iNEWS Connection

If your system is configured to connect to an Avid iNEWS server, complete the following steps.

To verify your iNEWS connection:

1. Select Log from the Layout menu in the top-right corner of the interface.





If you receive an error message indicating "This version if Interplay Central is not authorized to connect to the configured iNEWS Server.", verify that the correct iNEWS Client version has been entered into the iNEWS "SYSTEM.CLIENT.VERSIONS" story. For more information, see "Adding the MediaCentral UX Version to Avid iNEWS" on page 31.

2. Double-click one of the iNEWS systems to verify the connection. If the connection is successful, a list of iNEWS assets should appear in the Assets pane (shown on right).

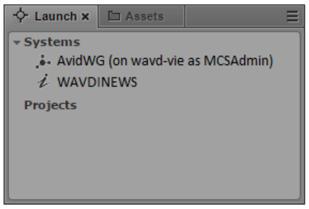
Verifying the Interplay Production and Avid Shared Storage Connections

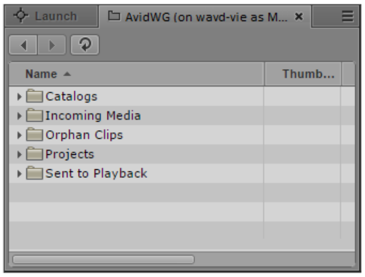
If your system is configured to connect to Interplay Production and Avid shared storage, complete the following steps.

To verify your Interplay Production and Avid shared storage connections:

1. Select Log from the Layout menu in the top-right corner of the interface.

   The Log layout will appear which consists of multiple default panes. The Launch pane (shown on left) lists available Interplay Production and iNEWS workgroups.





2. Double-click on AvidWG to verify the connection. If the connection is successful, a list of Interplay Production assets should appear in the Assets pane (shown on right).
3. Navigate through the assets tree to find a piece of media to play. Alternatively, the Search function can be used to find an asset.
4. Once you have found an asset, double-click on it to load it into the Media pane.
5. Click the Play button in the Media pane to verify playback.

Configuring Send To Playback Settings

If your workflow includes a Send To Playback (STP) component, configure and test those settings now. Depending on your workflow, one or more of the following are required:

- Interplay Transcode Provider – Required for STP Profiles using stereo audio tracks (audio mixdown) or for sequences with dissolves (video mixdown).
- Interplay STP Encode Provider – Required for workflows that include Long GOP media.
- Interplay Transfer Engine – Required for workflows that use non-Avid servers in their STP workflow such as Harmonic Omneon or Grass Valley K2. Interplay Transcode and STP Encode could also be required in this workflow.

To configure the Send To Playback settings:

1. In the Settings pane, select **Send to Playback**.
2. Click the plus sign '+' in the upper-right corner of this window to create a new profile.
3. Configure the profile settings:
   a. Name: Give the profile a name. Special characters and spaces are allowed if desired.

      Example: To AirSpeed

   b. Individual Device or Studio: Select the appropriate radio button.

      A "Studio" is a group of AirSpeed servers configured with a similar naming convention. The Studio is presented to the user as a single device. When a sequence is sent to the AirSpeed Studio, the media is sent to all AirSpeed servers simultaneously. This provides redundancy for on-air operations.

   c. Servers: This pull-down list is populated by the servers entered in the Interplay Administrator. Select a server from this list.

   d. Playback Device:

      - When selecting an AirSpeed, you will see AirSpeed and AirSpeed-HD options. The –HD options are valid if working with Long GOP media. Select an appropriate option for this profile.
      - When selecting a Transfer Engine, you will see the profiles configured on that server. Select an appropriate option for this profile.

   e. Video Options:

      - Long GOP: Select Long GOP if this profile will be used to transfer Long GOP media (XDCAM HD).
      - Accelerated STP: If you select both Long GOP and AirSpeed, the Accelerated STP option is activated. This option enables Play While Transfer (PWT).

- AirSpeed: Select this option if transferring to an AirSpeed (classic), AirSpeed Multi Stream, or AirSpeed 5000 / 5500.
- Dalet: Select this option if transferring to a Dalet system.

f. Video Target Resolution: Select a target resolution from the pull-down menu. The target device must match this setting. Make sure to match the settings specified on the target device.

g. Video Frame Rate: Select a frame rate from the pull-down menu. Make sure to match the settings specified on the target device.

Example: If using XDCAM-HD 50 mbps 1080i 60, select 59.94. If using 1080i 59.94 material, use 29.97.

h. Audio Target Sample Rate: This is always configured for 48k.

i. Audio Target Bit Depth: Select the bit depth (16 or 24) for your target device. Make sure to match the settings specified on the target device.

j. Audio Target Mixdown Mode: Select the type of audio output you want. Options are: Stereo or Direct Out.

k. Interplay | Production ISIS Workspace: Select a workspace for storing media that results from an audio mixdown or an STP Encode operation.

4. Click Apply.
5. If desired, create additional STP profiles.
6. Adjust STP Permissions as needed. This feature adds the ability to allow only certain user groups to send assets to the playback. If the STP Permissions section is left blank, all groups maintain the ability to STP.

   If you made any adjustments, click the Apply button once complete.
7. Once you have configured all required STP profiles, test your work by completing a Send To Playback test. See the Avid MediaCentral | UX User's Guide for information on creating a sequence within MediaCentral and sending media to playback.

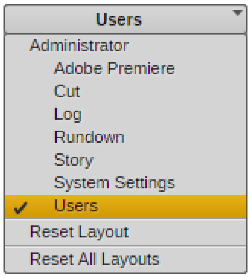
Importing Domain Users

If your workflow includes signing into MediaCentral UX as a domain user, review the information below to configure settings and import domain users into MediaCentral.

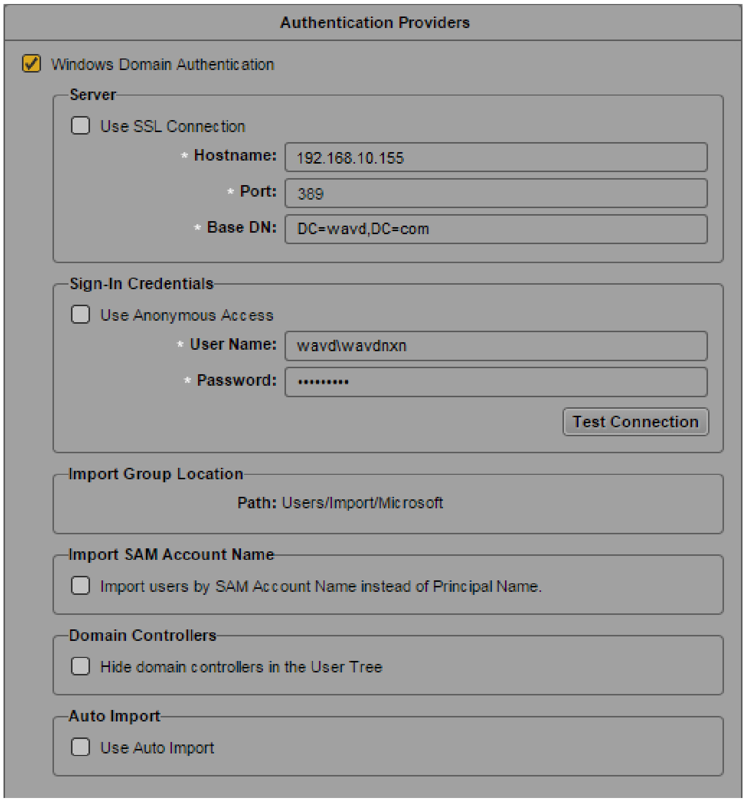
For more information about any of these settings, see the *Avid MediaCentral | UX Administration Guide*.

To import domain users:

1. While logged in as the Administrator, select Users from the Layout selector.



2. Double-click the top-level “Users” folder in the user tree on the left. The Authentication Providers settings will appear on the right.
3. 3.Enable the check box for “Windows Domain Authentication”.



Authentication Providers

☑ Windows Domain Authentication

Server

☐ Use SSL Connection

* Hostname: 192.168.10.155

* Port: 389

* Base DN: DC=wavd,DC=com

Sign-In Credentials

☐ Use Anonymous Access

* User Name: wavd\wavdnxn

* Password: •••••••••

Import Group Location

Path: Users/Import/Microsoft

Import SAM Account Name

☐ Import users by SAM Account Name instead of Principal Name.

Domain Controllers

☐ Hide domain controllers in the User Tree

Auto Import

☐ Use Auto Import

4. Configure the following settings:
   a. Use SSL Connection: If your site uses Secure Sockets Layer (SSL) technology, select this option.
   b. Hostnames: Enter the hostname, FQDN or IP address of a Domain Controller (DC) containing the user database. If multiple Domain Controllers are desired, separate each with a comma.
   c. Port: Enter the port used to communicate to the DC. The standard default port is 389. The SSL default port is 636.
   d. Base DN: The Base DN is the “root location” where the import of the user tree should be started.

      How you type the Base DN depends on how your Active Directory is configured and which domains you want to authenticate from. If you want to authenticate from multiple sub-domains, set the common root of the sub-domains instead of the Base DN of a specific domain. Examples:

      - DC=company,DC=com
      - DC=company,DC=division,DC=com
      - CN=Domain Users,OU=Organizational Unit, DC=company,DC=com

e. Sign-In Credentials:

- If applicable, select “Use Anonymous Access”. Selecting this will disable the user/ password fields.
- Alternatively, enter a user and password for a domain user that has appropriate access to the Active Directory user database. The user should be in the form of: domain\user

  Example: wavd\wavdnxn

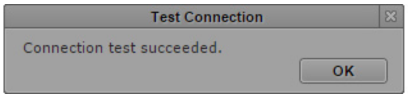
f. Import Group location: This is the location in the MediaCentral user tree where imported domain users will be located.

g. Import SAM Account Name: (Optional) If your facility uses SAM Account Names instead of the newer Active Directory Principal Names, select “Import users by SAM Account Name instead of Principal Name.” This configuration is specifically for those users who are used to logging into Interplay Production with the older Windows Domain style login.

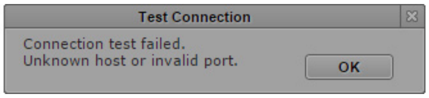
h. Domain Controllers: Select this check box to hide Domain Controllers in the import window.

i. Auto Import: Select this option if you want to automatically import new users from this Windows domain.

5. Click the “Test Connection” button. This will verify if the settings you have entered are valid. A pop-up window will indicate success or failure.



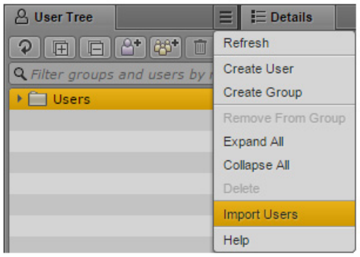
Connection test succeeded.

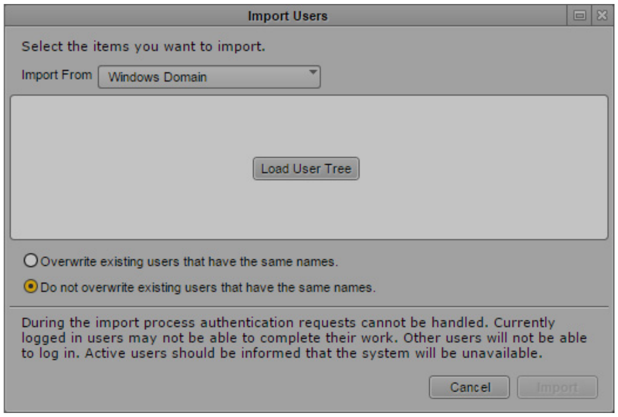


Connection test failed.
Unknown host or invalid port.

6. If your settings are valid, click Apply to save the information.
7. Click the menu button in the User Tree pane and select Import Users.

   The Import Users dialog box opens.





Select the items you want to import.

Import From: Windows Domain

○ Overwrite existing users that have the same names.

● Do not overwrite existing users that have the same names.

During the import process authentication requests cannot be handled. Currently logged in users may not be able to complete their work. Other users will not be able to log in. Active users should be informed that the system will be unavailable.

8. Select whether or not you want to overwrite existing users that have the same user names.

   In most cases, especially when reimporting, select “Do not overwrite existing users that have the same names.” This option preserves any existing user settings.

9. Click the Load User Tree button.

   A bar displays the progress while the user tree is loading. When the loading is complete, the root of the user tree appears.

10. Select the users or groups you wish to import and click the Import button. The users are imported into MediaCentral.

When users are imported into MCS, the user data is stored in the local user database. The fields in this database have a maximum limit of 255 characters. LDAP allows for some fields such as the "Distinguished Name" (DN) to be longer than 255 characters. If you find that some users are not imported into MCS, verify that none of the fields associated with the domain user are longer than 255 characters.

Creating Local Users and Assigning Roles

If desired, create additional non-domain user accounts within MediaCentral UX. This could be useful if you have a guest user or contractor that may only need access to MediaCentral UX for a short time.

You will also want to assign roles to the users or groups you have created either manually or through domain import. See the *Avid MediaCentral | UX Administration Guide* for more information about user creation and role assignment.

Continuing the Installation

Depending upon your workflow, proceed to one of the following sections as applicable:

- To configure a clustered environment, see "Clustering" on page 118.
- Configure "Sharded MongoDB" on page 129.

  This section is required for all cluster and multi-zone configurations.
- Complete the steps for "Verifying the Installation" on page 154.

  This section must be completed for all installations.
- To edit Closed Captioning data, see "Closed Captioning Service" on page 166
- To use Customizable Logging, see "Customizable Logger" on page 173.
- If integrating with an Avid Maestro server, see "Maestro UX Plug-In" on page 184.
- To add the Assignments Pane to MediaCentral UX, see "Assignments Pane" on page 204.
- To integrate with Interplay MAM systems, see "MAM Connector" on page 211.
- If configuring a multi-zone environment, see "Multi-Zone" on page 221.
- If adding Media Distribute, refer to the *Media | Distribute Installation and Configuration Guide* for detailed installation instructions.
- If your installation requires Indexed searching, refer to the *Media | Index Installation and Configuration Guide* for detailed installation instructions.

Review the *Avid MediaCentral | UX Administration Guide* and the *Avid MediaCentral | UX User's Guide* for additional information on customizing your base installation.

Configuring MCS for Interplay MAM

Prior to integrating MediaCentral Platform Services with an Interplay MAM system, verify that the MAM servers have been configured for MediaCentral. Some configuration steps:

- Configuring permissions to allow access to MAM storage
- Configuring the MCS hostname on the MAM server

For instructions on this aspect of setup and configuration, see the Interplay MAM documentation.

Mounting MAM Storage

For MCS to play Interplay MAM media, the filesystem containing the MAM proxies must be mounted on the MCS servers. Volume mounting is completed at the operating system level using standard Linux commands (e.g. mount). To automate the mounting of the MAM filesystem, create an entry in `/etc/fstab`.

Some proprietary storage solutions may require that you install and configure proprietary filesystem drivers or client software. Consult the documentation for the storage solution to be used by the Interplay MAM system.

To determine the correct path to be mounted, examine the path associated with the MAM essence pool to which MCS is being given access. This is found in the Interplay MAM Administrator interface under the Essence Management Configuration tab. Look for the “MORPHEUS” entry and tease out the path information. It is likely that MCS has been given access to more than one MAM essence pool. Be sure to mount all the associated filesystems.

When connecting to non-Avid shared storage, make sure that the MCS “maxmin” user has read access to the storage device. Failure to do so can lead to the inability to play assets through MediaCentral UX. Verifying user access can be accomplished through one of the following methods:

- Grant read access to the maxmin user on the remote storage system.
- Mount the storage in `/etc/fstab` with options to specify the maxmin account.

  For example, the following entry to the `/etc/fstab` file specifies the maxmin user with its user ID (UID) and group ID (GID) values:

  ```
  //wavd-iso/MAM/Archive cifs /storage
  ro,user=mam_service,passwd=Avid123,forceuid,uid=495,forcegid,gid=492
  ```

  You can verify the UID and GID on your MCS server using the Linux id command: `id maxmin`

For more information on mounting MAM storage, see the Interplay MAM documentation.

Configuring the ACS Gateway Access Port

If you are integrating with Interplay MAM V5.6, verify that the correct port has been entered in the Secure Gateway Port setting on the MAM server.

For more information, see “Configuring Interplay | MAM for Use with MediaCentral | UX” in the *MAM Installation Manual* v5.6 or later.

Configuring the MediaCentral User Interface

By default, the MediaCentral UI contains functionality for all the MCS solutions it supports. Functions that are not required for your installation should be removed. If you are configuring a cluster, this step only needs to be completed on the master and slave nodes, but it is good practice to run the configurator on all nodes. This step can be completed on all nodes concurrently.

For additional details on this process, see "Updating the MediaCentral UX Configuration" on page 91.

Configuring a Custom Audio-only Graphic (optional)

When loading an audio-only asset in the Media pane, an audio waveform graphic is displayed to alert users that the asset does not contain a video track.

If desired, sites can replace the default audio waveform graphic with a customized image by replacing the audioOnlyImage720.png file located at: `/var/www/html/player/static/images/`

Creating the MAM System User

When integrating with Interplay MAM, a specialized user needs to be created within MediaCentral.

If you are configuring an MCS cluster, complete this step on the Master Node only.

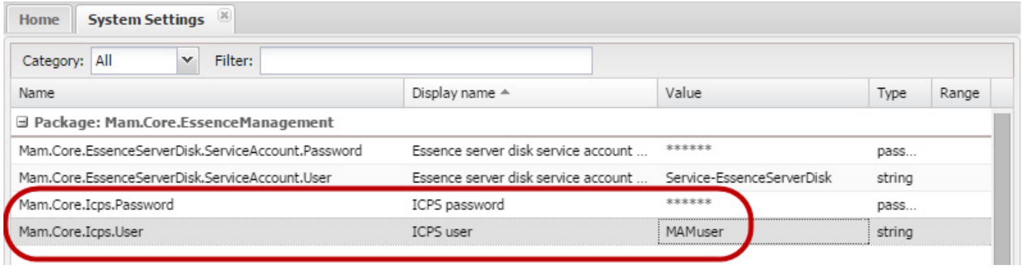
To create the MAM system user:

1. With the MCS server up and running, sign into MediaCentral as the Administrator user.

   For details, see "Signing into MediaCentral UX" on page 92.
2. Select Users from the Layout selector.
3. Create a special role for the MAM user by clicking on the Create Role button in the Roles pane.
4. Click the Create Role button.
5. In the Details pane, type the properties for the new role:
   - Role name (e.g. MAM)
   - Advance License
   - Do not assign the MAM role any layouts
6. Click Apply to save your changes.

   The new MAM role is added to the Roles pane.
7. Create the MAM system user by clicking the Create User button.
8. In the Details pane, type the properties for the new user:
   - User name (e.g. MAMuser)
   - Password
   - Uncheck "User must change password at next sign-in"
   - Check "User cannot change password
9. Drag the MAM role from Roles pane to the Role section of the Details pane for the new user.
10. Click Save to save your changes.

11. Ensure the System Settings on the Interplay MAM system are configured to make use of the assigned user name and password. Example:



Name	Display name	Value	Type	Range
Package: Mam.Core.EssenceManagement				
Mam.Core.EssenceServerDisk.ServiceAccount.Password	Essence server disk service account ...	******	pass...	
Mam.Core.EssenceServerDisk.ServiceAccount.User	Essence server disk service account ...	Service-EssenceServerDisk	string	
Mam.Core.Icps.Password	ICPS password	******	pass...	
Mam.Core.Icps.User	ICPS user	MAMuser	string	

See the *Avid MediaCentral | UX Administration Guide* for more information about user creation and role assignment.

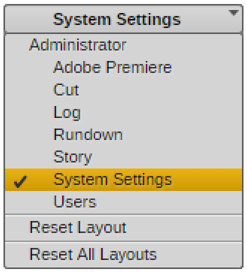
Configuring the MCS Player

Configuring the MCS Player setting allows you to monitor connections to the player through the MediaCentral System Settings > MCPS > Load Balancer page.

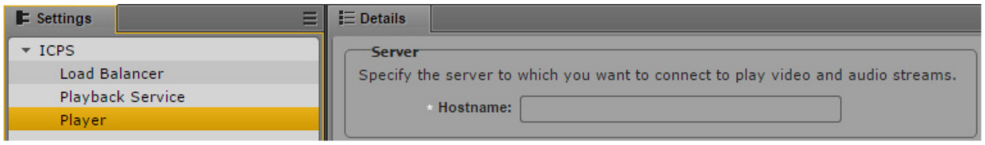
If you are configuring an MCS cluster, complete this step on the Master Node only.

To configure the MCS Player:

1. While logged in as the Administrator, select System Settings from the Layout selector.
2. In the Settings pane, select MCPS > Player.



3. In the Serve r> Hostname field, enter the Fully Qualified Domain Name (FQDN) of the MCS server.



Specify the server to which you want to connect to play video and audio streams.

Example: wavd-mcs01.wavd.com

If you are in the process of setting up the first server in a cluster, enter the FQDN of the server you are working on (node1 of the cluster). Later in the process, you will update this field with the virtual cluster hostname.

4. Click Apply to save your changes.

Enabling Remote Playback

MediaCentral Platform Services v2.5 introduced an alternative configuration for playback support of remote assets in MAM configurations. In previous releases, each MCS system required external storage for the MAM assets. Media was transferred between the systems resulting in increased storage costs and network bandwidth.

MediaCentral 2.5 and later allows for low-res proxy media to be streamed to the remote systems and stored on a local cache. This eliminates the need to replicate media at the remote locations.

Note the following when considering this configuration:

- All MCS systems must be connected in a multi-zone configuration.
- This workflow is currently available for Frame-based playback only.

Enabling the alternative configuration requires the adjustment of two files on the MCS servers.

Additionally, system administrators can streamline playback requests by making a change to a system configuration file. When a remote playback request is issued, the remote system normally validates the user's session ID with the User Management Service (UMS). Adding one or more trusted hosts to the edit.cfg file bypasses the session ID check on the remote system which results in accelerated processing of the playback request. This is an optional configuration change for sites that wish to reduce latency for remote playback requests.

To enable MAM remote playback:

1. Log into the MCS server (at the Linux prompt) as the root user.
2. Open the `edit.cfg` file with a text editor (such as vi):

   ```
   vi /usr/maxt/maxedit/etc/edit.cfg
   ```
3. Locate the line under the `<general>` category for `<enable_remote_proxy>`.
4. Change the default value from false to true. For example:

   ```
   <enable_remote_proxy>true</enable_remote_proxy>
   ```
5. Save and exit the vi session. Press <ESC> and type: `:wq`
6. Open the `fl_xmd.cfg` file with a text editor (such as vi):

   ```
   vi /usr/maxt/maxedit/etc/fl_xmd.cfg
   ```
7. Locate the line in the file that reads `<enable_remote_proxy>`.
8. Change the default value from false to true. For example:

   ```
   <enable_remote_proxy>true</enable_remote_proxy>
   ```
9. Save and exit the vi session. Press <ESC> and type: `:wq`
10. If your MCS server is part of a clustered configuration, repeat the above steps on all cluster nodes.
11. Once complete, the AvidAll service must be restarted:
    - For a single MCS server:

      ```
      service avid-all restart
      ```
    - For a cluster configuration:

      ```
      crm resource restart AvidAllEverywhere
      ```

To create a list of trusted servers:

1. Log into the **remote** MCS server (at the Linux prompt) as the root user.
2. Open the `edit.cfg` file with a text editor (such as vi):

   ```
   vi /usr/maxt/maxedit/etc/edit.cfg
   ```

3. Locate the line under the `<general>` category for `<trusted_hosts></trusted_hosts>`.
4. Add the host names or IP addresses of your local MCS server(s) between the angled brackets. If you are adding multiple servers, separate each entry with a comma. For example:

   ```
   <trusted_hosts>wavd-mcs01,wavd-mcs02,wavd-newyork</trusted_hosts>
   ```

   In the example above, the list of trusted servers includes a 2-node cluster in one zone (wavd-mcs01,wavd-mcs02) and a single server from a second zone (wavd-newyork). These two zones can now play back media from the remote zone without first validating the user session with the User Management Service (UMS).

   Only trusted servers added to this configuration file are granted access without validation.

If the local system is a cluster, all cluster nodes ***must*** *be added to the edit.cfg file of the remote zone as the player service is load-balanced across all cluster nodes.*

5. Save and exit the vi session. Press <ESC> and type: **`:wq`**
6. If your MCS server is part of a clustered configuration, repeat the above steps on all cluster nodes.
7. Once complete, the AvidAll service must be restarted:
   - For a single MCS server:

     ```
     service avid-all restart
     ```

   - For a cluster configuration:

     ```
     crm resource restart AvidAllEverywhere
     ```

8. If playback is bi-directional (the remote system needs to play back media on the local server), use the process above to edit the configuration file on the local system as well.

Continuing the Installation

Depending upon your workflow, proceed to one of the following sections as applicable:

- To configure a clustered environment, see “Clustering” on page 118.
- Configure “Sharded MongoDB” on page 129.

  This section is required for all cluster and multi-zone configurations.
- Complete the steps for “Verifying the Installation” on page 154.

  This section must be completed for all installations.
- To use Customizable Logging, see “Customizable Logger” on page 173.
- If integrating with an Avid Maestro server, see “Maestro UX Plug-In” on page 184.
- To add the Assignments Pane to MediaCentral UX, see “Assignments Pane” on page 204.
- To integrate with Interplay MAM systems, see “MAM Connector” on page 211.
- If configuring a multi-zone environment, see “Multi-Zone” on page 221.

- If adding Media Distribute, refer to the *Media | Distribute Installation and Configuration Guide* for detailed installation instructions.
- If your installation requires Indexed searching, refer to the *Media | Index Installation and Configuration Guide* for detailed installation instructions.

5 Clustering

Chapter Overview

The purpose of this chapter is to guide you through the creation and configuration of a multi-server MCS cluster.

The following table describes the topics covered in this chapter:

Step	Task	Time Est.
1	Cluster Overview	varies
	Overview information and prerequisite checks for building the cluster.	
2	Configuring the Player System Setting	5 min
	Process for updating the MediaCentral Player System Setting.	
3	Configuring DRBD	15 min
	Configure DRBD to replicate the PostgreSQL database across the master and slave nodes.	
4	Starting the Cluster Services on the Master Node	15 min
	Begin the cluster configuration on the Master node.	
5	Adding Nodes to the Cluster	150 min
	Connect the slave node and any additional load balancing nodes to the cluster.	
6	Replicating the File Caches using GlusterFS	10 min
	Configure Gluster to mirror the /cache directories, so each server in the cluster can easily use material transcoded by the others.	

Cluster Overview

A cluster is a group of two or more MCS servers that work together to provide high-availability, load balancing and scale. Each server in a cluster is called a “node”. During the cluster configuration, one server is identified as the Master node. The master node owns multiple databases and important services or “cluster resources” that enable MCS and the cluster to operate. The second server in the cluster is called the Slave node. The slave node provides high-availability of some specialized MCS services and increases scale by load balancing certain client requests such as media playback. In the event of a fail-over, the slave node becomes the new master and owner of the MCS databases and resources. Additional “Load Balancing” nodes (3+) can be added to the configuration. These servers do not participate in high-availability; they provide load balancing and system scaling only.

Throughout this document, cluster nodes are identified as the following:

- Master Node (node1): wavd-mcs01 / 192.168.10.51
- Slave Node (node 2): wavd-mcs02 / 192.168.10.52
- Load Balancing Nodes (node3, node4): wavd-mcs03 / 192.168.10.53, wavd-mcs04 / 192.168.10.54

Once the cluster is created, external systems no longer communicate directly with individual nodes, as they would with a single-server configuration. All traffic is processed through a virtual cluster hostname and IP address. This allows the clients to connect to the cluster no matter which server is the current Master. Throughout this process the virtual cluster will be identified by the following:

- Virtual Cluster Name / IP: wavd-mcs / 192.168.10.50

Prior to proceeding with the cluster process, confirm the following:

- You have fully configured and tested the Master node. All other nodes should be configured through the Software Installation chapter of this document.
- Hostnames and IP addresses have been assigned to each cluster node (static IP’s are required for cluster configurations).
- The primary network interface on each node must have the same name (e.g. eth0, em1, etc).
- You have decided on a virtual cluster hostname and a unicast IP address (to be used for communication between cluster and external systems – such as a MediaCentral UX client).
- You have decided on a multicast IP address (to be used for internal communication between the cluster nodes). If necessary, a unicast IP can be used. However, specifying a unicast IP requires additional configuration.

  For more information, see “Unicast Support in Clustering” on page 265.
- All hostnames and IP addresses, including the cluster’s virtual name and IP, resolve normally through DNS.

For a complete list of installation prerequisites, see the *Avid MediaCentral Platform Services Installation Pre-Flight Checklist* on the Avid Knowledge Base.

For detailed information on MCS Clusters, see the *MediaCentral Platform Services Concepts and Clustering Guide*.

http://avid.force.com/pkb/articles/en_US/user_guide/Avid-MediaCentral-Documentation

Configuring the Player System Setting

When configuring and testing the Master node, you entered the Fully Qualified Domain Name (FQDN) of the server in the MediaCentral System Settings. Prior to configuring the cluster, you need to alter this setting to reflect the **cluster's** FQDN.

To reconfigure the Player settings:

1. Using Chrome or another qualified browser, sign into MediaCentral UX as the Administrator.
2. Select System Settings from the Layout pull-down menu.
3. In the Settings pane, select MCPS > Player.
4. In the Server field, enter the Fully Qualified Domain Name (FQDN) of the virtual MCS server.

   Example: wavd-mcs.wavd.com
5. Click Apply to save the setting.
6. Sign out of MediaCentral UX and close the web browser.

Configuring DRBD

In a clustered configuration, MCS uses the open source Distributed Replicated Block Device (DRBD) storage system software to replicate the PostgreSQL database between the Master and Slave nodes. Even in a cluster with more than two nodes, DRBD runs on the Master and Slave nodes only.

Clearing the SDA2 Partition

If you are installing MCS on known HP or Dell hardware and used the MCS Installation USB Drive to install the server, proceed directly to "Running the drbd_setup Script" on page 121. If you are installing MCS in a virtual environment or you have manually installed RHEL on non-HP or Dell hardware, you might encounter the following error when configuring DRBD:

```
Device size would be truncated, which would corrupt data and result in 'access
beyond end of device' errors.
You need to either
   * use external meta data (recommended)
   * shrink that filesystem first
   * zero out the device (destroy the filesystem)
Operation refused.
```

This error indicates that the drbd_setup script encountered an issue with the sda2 partition. The script expects to find an empty 20GB sda2 partition. If you have created this partition in a virtual environment or on non-HP or Dell hardware, the partition might not be empty. Use the following process to wipe the sda2 partition. Complete this process on the master and slave nodes only.

To initialize the DRBD partition:

1. Ensure that the drbd service is not running by stopping the service:

   ```
   service drbd stop
   ```
2. Navigate to the drbd directory:

   ```
   cd /etc/drbd.d
   ```
3. If present, delete the "r0.res" file located in this directory:

```
rm r0.res
```

4. Enter the following command to “zero” the sda2 partition:

```
dd if=/dev/zero of=/dev/sda2 bs=512k count=10000
```

This command is destructive, so take care when entering the command.

The command might take a few minutes to complete. There is no indication of progress during this period. Once complete a message similar to the following is displayed:

```
10000+0 records in
10000+0 records out
5242880000 bytes (5.2 GB) copied, 80.0694 s, 65.5 MB/s
```

5. Once completed on both master and slave nodes, proceed to “Running the drbd_setup Script” on page 121.

Running the drbd_setup Script

The following process configured DRBD on the Corosync cluster master and slave nodes.

To configure DRBD:

1. On the Master node, navigate to the directory containing the drbd_setup script:

```
cd /opt/avid/cluster/bin
```

2. Run the drbd_setup script:

```
./drbd_setup primary_host="master hostname" secondary_host="slave hostname"
```

The quotes are required in this command. The hostnames in this command are **case sensitive** and must **exactly** match the hostnames for the master and slave nodes defined during the Linux setup process. DRBD requires you to enter the short hostname and not the FQDN.

The period-slash “./” in this command tells Linux to look for the script in the current directory.

The following provides an example of the command and the associated switches and variables:

```
drbd_setup
[primary_host="<hostname>"] [secondary_host="<hostname>"]
{[primary_ip="<ip>"] [secondary_ip="<ip>"]}
{[primary_disk="<device>"] [secondary_disk="<device>"]}
```

- **primary_host**: Host name (e.g. wavd-mcs01) of the machine to serve as Master node for DRBD.
- **secondary_host**: Host name (e.g. wavd-mcs02) of the Slave node (the machine to serve as fail-over for DRBD).
- **primary_ip**: Optional. IP address (e.g. 192.xxx.xxx.xxx) of the Master node. Helpful when host primary_host specified does not resolve.
- **secondary_ip**: Optional. IP address (e.g. 192.xxx.xxx.xxx) of the Slave node. Helpful when secondary_host does not resolve.
- **primary_disk**: Optional. Name of the disk device reserved for DRBD on the Master node (/dev/sda2 by default).
- **secondary_disk**: Optional. Name of the disk device reserved for DRBD on the Slave node (/dev/sda2 by default).

The primary_disk and secondary_disk parameters are provided for special cases in which the partitions reserved for DRBD are in a non-standard location. In most cases, the default value of /dev/sda2 is correct.

3. Depending on your configuration, multiple informational or error messages could appear:

   - If you receive an error message indicating that the IP addresses cannot be identified using the host names, add the “primary_ip” and “secondary_ip” switches to the command:

     ```
     ./drbd_setup primary_host="master hostname" secondary_host="slave
     hostname" primary_ip="ip of master node" secondary_ip="ip of slave node"
     ```

If you do not know why the hostnames could not be identified, investigate the reason for the problem. Hostname resolution is critical to many aspects of MCS.

   - If you receive error messages indicating the bus is not running or a path does not exist, these can be ignored:

     ```
     error: bus is not running

     error: Given --path is not exist:
     ```

   - If you receive the following message, it indicates that the DRBD setup script has found the 20GB partition set aside for it and is about to take ownership of it. If this occurs, type **yes** (the whole word) at the prompt to continue with the setup:

     ```
     Found some data
     ==> This might destroy existing data! <==

     Do you want to proceed?
     [need to type 'yes' to confirm]
     ```

4. The system responds, and waits for the other DRBD node, with output similar to the following:

   ```
   Writing meta data...
   initializing activity log
   NOT initializing bitmap
   New drbd meta data block successfully created.
   Waiting for secondary node...
   ```

5. On the Slave node, navigate to the directory containing the drbd_setup script:

   ```
   cd /opt/avid/cluster/bin
   ```

6. On the Slave node, run the same drbd_setup command that you ran on the Master node.

   The Master node responds with output similar to the following:

   ```
   Secondary node found
   Node initialized with role: Primary
   Stopping postgresql-9.1 service:                          [  OK  ]
   Stopping mongod:                                          [  OK  ]
   Stopping redis-server:                                    [  OK  ]
   mke2fs 1.41.12 (17-May-2010)
   Filesystem label=
   OS type: Linux
   Block size=4096 (log=2)
   Fragment size=4096 (log=2)
   Stride=0 blocks, Stripe width=0 blocks
   1310720 inodes, 5242711 blocks
   262135 blocks (5.00%) reserved for the super user
   First data block=0
   Maximum filesystem blocks=4294967296
   160 block groups
   32768 blocks per group, 32768 fragments per group
   8192 inodes per group
   ```

```
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632,
        2654208, 4096000

Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 21 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
partition mounted at  /mnt/drbd]
```

A fail message might appear when the drbd_setup script tries to start PostgreSQL. This is normal.

Finally, information indicating that synchronization is underway appears in the output of the master node (similar to the following). The synchronization process can take some time, since DRBD replicates at the block level.

```
Node synchronization started
5% synchronized
…
55% synchronized
97% synchronized
Node synchronization finished
```

7. Wait until node synchronization is completed before proceeding to the next step.

Starting the Cluster Services on the Master Node

MCS supports both multicast and unicast for intra-cluster communication. The body of this guide provides instructions for configuring a cluster in a multicast environment (standard configuration). However, multicast requires multicast enabled routers. If your network does not support multicast, see "Unicast Support in Clustering" on page 265 for details on altering the configuration.

To configure the cluster master node:

1. On the **Master node only**, assign the cluster multicast IP address. This is the IP that the cluster will use for communication between the nodes.

   a. If your network has no other multicast activity, the default multicast address of 239.192.1.1 is assumed in the following command:

   ```
   /opt/avid/cluster/bin/cluster setup-corosync --corosync-bind-
   iface=interface --rabbitmq_master="master hostname"
   ```

   b. If your network includes multicast activity (perhaps a second MCS system is already on the network), specify a custom multicast address with the following command:

   ```
   /opt/avid/cluster/bin/cluster setup-corosync --corosync-bind-
   iface=interface --corosync-mcast-addr="multicast address" --
   rabbitmq_master="master hostname"
   ```

The following provides an example of the command and the associated switches and variables:

```
cluster setup-corosync
[corosync-bind-iface =<interface>]
{[--corosync-mcast-addr="<ip>"]}
{[--rabbitmq_master="<device>"]}
```

--corosync-bind-iface: Identifies the name of the primary network interface. In an HP server, this is generally "eth0". In a Dell server, this is generally "em1" for 1 Gb connections or "p1p1" / "p2p1" for 10 Gb connections (depending on which slot the card 10 Gb card has been installed). For Interplay MAM configurations with port bonding, this is generally "bond0". Quotes are not required with this variable.

--corosync-mcast-addr: In configurations that do not use the default multicast address of 239.192.1.1, this command can be used to specify a custom multicast address. Quotes are required with this variable.

--rabbitmq_master: This specifies the (short) hostname of the Master node in the cluster (e.g. wavd-mcs01). This should be the same as the DRBD Master node specified in the drbd_setup process. Quotes are required with this variable.

As of MCS v2.0, this command will not accept a multicast address outside of the 239.0.0.0/8 range. If specifying a non-239.x.x.x, you will see an error: "Multicast IP is not in subnetwork 239.0.0.0/8".

Messages appear echoing the Corosync network binding process; followed by messages indicating that services are being stopped. At the end of the process, you are informed that the Corosync cluster engine has successfully started [OK].

The following is sample output:

```
bind_iface=eth0 bind_network=192.168.10.51 mcast_addr=239.192.1.1
Avid Service: edit fl_xmd: no process killed
..
...
Starting Corosync Cluster Engine (corosync):[  OK  ]
Starting Pacemaker Cluster Manager:[  OK  ]
```

You may notice the following text appear during this process:

```
Clustering node rabbit@nodename with rabbit@nodename...
Error: cannot_cluster_node_with_itself
Starting node rabbit@nodename....
…done
```

```
Failed to join cluster, exiting!!
```

This message can be ignored as it simply indicates that this is the first node in the RabbitMQ cluster.

2. On the **Master node only**, assign the cluster’s virtual unicast IP address. This is the IP that the cluster will use for communication with clients and external systems:

```
/opt/avid/cluster/bin/cluster setup-cluster --cluster_ip="cluster IP address" --pingable_ip="router IP address" --cluster_ip_iface="interface" --admin_email="comma separated e-mail list" --drbd_exclude="comma separated list of non-DRBD nodes"
```

The following provides an example of the command and the associated switches and variables:

```
cluster setup-cluster
{[--cluster_ip="<cluster IP address>"]}
{[--pingable_ip="<router IP address>"]}
{[--cluster_ip_iface="<interface_name>"]}
{[--admin_email="<comma separated e-mail list>"}]
{[--drbd_exclude="<comma separated list of non-DRBD nodes>"}]
```

--cluster_ip: Identifies the unicast virtual IP address assigned to the cluster (e.g. 192.168.10.50).

--pingable_ip: This is an IP address that will always be available on the network - for example, the IP address of your default gateway (e.g. 192.168.10.1).

-- cluster_ip_iface: Identifies the name of the primary network interface. In an HP server, this is generally “eth0”. In a Dell server, this is generally “em1” for 1 Gb connections or “p1p1” / “p2p1” for 10 Gb connections (depending on which slot the card 10 Gb card has been installed). For Interplay MAM configurations with port bonding, this is generally “bond0”.

--admin_email: This is a comma separated list of e-mail addresses to which cluster status notifications are automatically sent. This command is not optional. If you do not want to receive e-mail notifications, enter a bogus email address.

At least one cluster administrator email address is mandatory (though not validated by the system). To change the email address later, see “Changing the Administrator E-mail Address” in the MediaCentral Platform Services Concepts and Clustering Guide.

--drbd_exclude: This is a comma separated list of the non-DRBD nodes in the cluster (e.g. wavd-mcs03, wavd-mcs04). This parameter prevents the non-DRBD nodes from running PostgreSQL. The comma-separated list of non-DRBD nodes must not contain any spaces between each entry, only a comma. The values must be entered as host names and not IP addresses. If you only have two nodes (master and slave), this switch can be eliminated from the command.

Quotes are required with each of the above variables.

Error messages appear indicating missing resources and attributes. For example:

```
ERROR: resource <resource name> does not exist
Error: performing operation: The object/attribute does not exist
```

These can be ignored.

Additional warning, error and info messages may also appear, similar to the following:

```
WARNING: 125: AvidConnectivityMon: specified timeout 20s for start is
smaller than the advised 60
ERROR: 125: rsc-options: attribute admin-email does not exist
INFO: 125: commit forced
```

These can also be ignored.

3. Restart the following services so they register correctly on the newly created instance of the message bus:

   ```
   service avid-acs-messenger restart
   ```

   ```
   service avid-aaf-gen restart
   ```

   ```
   service avid-acs-mail restart
   ```

4. Now that the clustering services are up and running on the master node, start the Cluster Resource Monitor tool:

   ```
   crm_mon
   ```

   This utility provides a “live view” of the cluster which can be useful as you add additional nodes to the cluster. Typing “crm_mon –f” will give you additional information about fail-counts. When necessary, press CTRL-C to exit crm_mon.

   For more information on the Cluster Resource Monitor, see the *MediaCentral Platform Services Concepts and Clustering Guide*.

If you are using a SSH tool such as PuTTY, open a second session to the Master cluster node and run the “crm_mon” monitoring tool in a dedicated window.

Adding Nodes to the Cluster

With the clustering services up and running on the Master node, add the other servers to the cluster.

If your network does not support multicast activity, see “Unicast Support in Clustering” on page 265 for details on altering the configuration.

This process assumes that you are adding nodes to a new cluster configuration. If you are adding nodes to an existing, fully configured cluster, refer to the process for “Adding Nodes to a Cluster” in the MediaCentral Platform Services Concepts and Clustering Guide.

For more information on the variables used with the “cluster setup-corosync” command referenced in this section, see “Starting the Cluster Services on the Master Node” on page 124.

To add nodes to the cluster:

1. On each of the non-master nodes in the cluster, complete one of the following:

   a. If your network has no other multicast activity, the default multicast address of 239.192.1.1 is assumed in the following command:

   ```
   /opt/avid/cluster/bin/cluster setup-corosync --corosync-bind-
   iface=interface --rabbitmq_master="master hostname"
   ```

   b. If your network includes multicast activity (perhaps a second MCS system), specify a custom multicast address with the following command:

   ```
   /opt/avid/cluster/bin/cluster setup-corosync --corosync-bind-
   iface=interface --corosync-mcast-addr="multicast address" --
   rabbitmq_master="master hostname"
   ```

As before, messages appear echoing the Corosync network binding process. The Avid UMS service is temporarily shut down. A message appears indicating the Corosync cluster engine has successfully started.

The following is sample output:

```
bindip=192.168.10.53/24 bind_iface=eth0 bind_network=192.168.10.0
mcast_addr=239.192.1.1

.....
Starting Corosync Cluster Engine (corosync):                    [  OK  ]
Starting Pacemaker Cluster Manager                              [  OK  ]
```

2. Restart the following services so they register correctly on the newly created instance of the message bus:

```
service avid-acs-messenger restart
```

```
service avid-aaf-gen restart
```

```
service avid-acs-mail restart
```

After this point, if you reconfigure any MediaCentral UX System Settings, the new settings are applied to the Master node only. Non-master nodes must be updated manually. On each non-master node, log in as root and run the following command: `service avid-all reconfigure`

Replicating the File Caches using GlusterFS

When a playback request is sent to an MCS server, the media is obtained from the storage system and is quickly transcoded into an alternate delivery format. The transcoded media is stored in the MediaCentral server’s `/cache` directory. In the case of a cluster, the transcoding is performed on the cluster node that received the playback request. To expedite playback of the same media for future playback requests (where the request may be handled by a different node), the contents of the `/cache` folder is automatically replicated to all cluster nodes. The replication is completed using GlusterFS, an open source software solution for creating shared file systems.

Cluster and Gluster are independent from each other. Multiple MCS servers require a Cluster but may not require Gluster. See the MediaCentral Platform Services Concepts and Clustering Guide for more information on Gluster configurations.

Versions of MediaCentral Platform Services prior to v2.5 require a multi-step process for configuring Gluster. MCS v2.5 introduces a custom script which expedites the process for configuring Gluster across the cluster nodes.

If for any reason you need to refer to the manual configuration process, see “Replicating the File Caches using GlusterFS” in the v2.4 MediaCentral Platform Services Installation and Configuration Guide.

Configuring GlusterFS

This process will create the Gluster volumes and configure the correct permissions for all directories.

To configure GlusterFS:

1. Verify that the Gluster daemon, glusterd, is running:

```
service glusterd status
```

If the service is not running, start it manually:

```
service glusterd start
```

Repeat this step on all nodes before proceeding to the next step.

2. Create the RHEL physical directories that Gluster will use to build its GlusterFS file system:

```
mkdir -p /cache/gluster/gluster_data_download
mkdir -p /cache/gluster/gluster_data_fl_cache
mkdir -p /cache/gluster/gluster_data_multicam
```

   Create these directories on all nodes before proceeding to the next step.

3. From the corosync master node, run the Gluster configuration script:

```
/opt/avid/cluster/bin/gluster_setup
```

   The process for configuring Gluster on the first node will take slightly longer than the other cluster nodes. Once the script is complete, you should receive a confirmation message:

```
Starting glusterd:                                          [  OK  ]

INSTALLATION OF GLUSTERFS FINISHED
```

4. Run the Gluster configuration script on all other cluster nodes. Run the script one node at a time, proceeding to the next node only after the previous node has finished.

5. Once you have run the script on all nodes, verify that you the nodes are aware of each other:

```
gluster peer status
```

   The system responds by indicating the number of peers, their host names and connection status, plus other information. Example:

```
Number of Peers: 1
Hostname: wavd-mcs02
Uuid: 220976c3-dc58-4cdc-bda3-7b2213d659fc
State: Peer in Cluster (Connected)
```

Testing the File Replication

Prior to continuing with the installation, verify that Gluster is replicating the caches correctly. This is completed by writing a file to one of the GlusterFS cache folders (e.g. /cache/download) on one servers and confirming that the file appears on all of the other servers.

To verify file replication:

1. From any node, use the Linux touch command to write two test files to the /cache directories:

```
touch /cache/download/test01.txt
touch /cache/render/test02.txt
```

2. On all other nodes, verify that the files have been replicated to the local /cache directories:

```
ls /cache/download/
ls /cache/render/
```

6 Sharded MongoDB

Chapter Overview

This chapter focuses on the creation of the sharded MongoDB environment.

The following table describes the topics covered in this chapter:

Task
Chapter Overview
Reviews some of the core concepts regarding a sharded Mongo configuration.
Configuring Sharded Mongo for a Single Server
Instructions for completing the installation on a single MCS server.
Configuring Sharded Mongo with an MCS Load-Balancing Node
Instructions for completing the installation on a MCS cluster consisting of three or more servers.
Configuring Sharded Mongo with a (non-MCS) Linux Arbiter
Instructions for completing the installation on a two-node MCS cluster with an external Linux-based arbiter.
Configuring Sharded Mongo with a Windows Arbiter
Instructions for completing the installation on a two-node MCS cluster with an external Windows-based arbiter.
Configuring Sharded Mongo in a Multi-Zone Configuration
Instructions for completing the installation in a multi-zone configuration.
Adding a Zone to a Sharded Mongo Multi-Zone Environment
Details the process of adding new nodes to an existing Sharded Mongo / multi-zone configuration.

Sharded MongoDB Overview

Sharded Mongo is a distributed database where copies or "shards" of the database exist on multiple servers. Originally introduced in version 2.6, MCS v2.9 adds a second sharded Mongo database which is configured somewhat differently from the first sharded Mongo implementation.

Sharded Mongo for avid-iam

The first sharded Mongo database introduced in MCS v2.6 is used by the "avid-iam" and "upstream" services to enable authentication of both Avid and third party "plugins" or "applications" in MediaCentral through a collection of APIs called the Avid Connectivity Toolkit.

Single-server deployments operate in a "sharded" environment, but only a single shard is present on the local server. Database redundancy and fault tolerant functionality is not available.

In an MCS cluster, the Corosync master and slave nodes each host a "shard" (copy) of the Mongo database. Although the database is located on the Corosync master and slave nodes, MongoDB uses its own internal mechanisms to provide high availability, separate from Corosync. In multi-zone environments, all zones are included in the sharded configuration with each zone hosting shards of both the local and remote databases. This creates a multi-zone sharded Mongo cluster that allows for database redundancy and faster access to each database.

When operating in a two-node Corosync cluster configuration, a third instance of Mongo is required to function as a tie-breaker in the event of an election. An election occurs if a node is down due to a network outage, power loss or other. This tie-breaking node is known as an "arbiter".

In a Corosync cluster consisting of three or more nodes, an MCS load-balancing node serves as the arbiter. If your configuration consists of only two nodes, a third instance of Mongo must be created on an external Linux or Windows box that has consistent network access to the cluster nodes.

Arbiters are not required for the avid-iam instance of sharded Mongo in single-server or multi-zone configurations. This is true even if your environment consists of a multi-zone configuration with only two single-server zones.

Arbiters do not host a database shard and consume a very limited amount of resources on the host system (less than 1% CPU usage). Their only purpose is to provide a vote in an election. Therefore the CPU, RAM and storage requirements are low. Arbiters can often be co-located on a Linux or Windows system whose primary resources are dedicated to other functions. Co-location examples include iNEWS servers and Interplay Production servers.

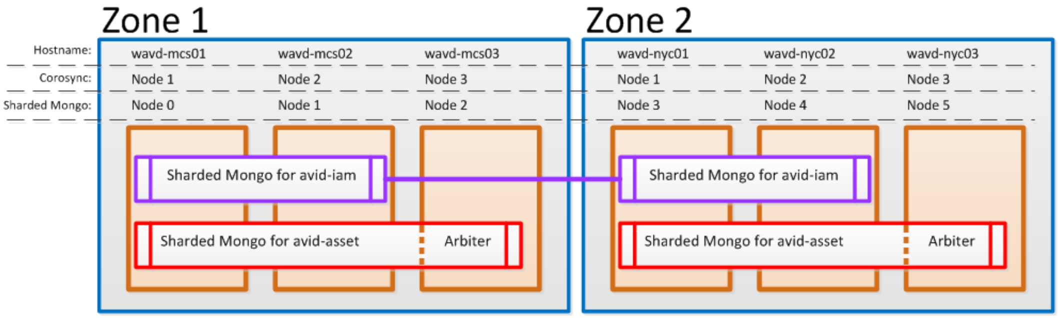
Do not install the MongoDB arbiter on clustered Interplay Production Engines.

Sharded Mongo for avid-asset

MCS v2.9 introduces two new services (avid-asset and avid-asset-gc) which provide an infrastructure for the "Mixed Sequence Editing" Technology Preview introduced in MCS v2.9 as well as for features planned in future releases. Sites that do not intend to enabled Mixed Sequence Editing must still enable this instance of sharded Mongo.

Beginning the Configuration

The primary difference between the two sharded Mongo deployments applies to multi-zone configurations. The avid-asset services are not multi-zone compliant. This means that even in a multi-zone environment, an arbiter is required for the sharded Mongo database used by the avid-asset service. Consider the following illustration:



The figure above shows a simple multi-zone configuration consisting of only two zones. Each zone includes a 3-node MCS cluster. As you can see, the original sharded Mongo configuration for avid-iam includes shards on the master and slave nodes of each zone. Since avid-iam is multi-zone aware, no arbiter is required. However the new instance of sharded Mongo for the avid-asset service is not multi-zone compliant and a standalone 2-node + arbiter configuration is required in each zone.

Although the deployments of sharded Mongo for avid-iam and avid-asset are different, the configuration process is completed using the same configuration scripts found in previous releases of MediaCentral Platform Services. The sharded Mongo services for avid-asset are configured and deployed at the same time as the avid-iam services. No additional steps or scripts are required, even for multi-zone environments.

When configuring sharded Mongo, all commands must be run from the same server (unless otherwise directed). Once the `.../ansible/hosts` and `.../ansible/hosts_vars/node<#>` files are created, this server is referred to as the sharded Mongo "management node".

If you plan to configure a multi-zone environment, complete the multi-zone configuration process prior to sharded Mongo. For details, see the chapter on "Multi-Zone" on page 221.

Refer to one of the following sections to create a sharded Mongo configuration applicable to your environment:

- Configuring Sharded Mongo for a Single Server
- Configuring Sharded Mongo with an MCS Load-Balancing Node
- Configuring Sharded Mongo with a (non-MCS) Linux Arbiter
- Configuring Sharded Mongo with a Windows Arbiter
- Configuring Sharded Mongo in a Multi-Zone Configuration
- Adding a Zone to a Sharded Mongo Multi-Zone Environment

For additional information on sharded Mongo including tools and troubleshooting information, see "Working with Sharded Mongo" on page 277.

For even more detail on this topic, see "MongoDB" in the *MediaCentral Platform Services Concepts and Clustering Guide*.

Configuring Sharded Mongo for a Single Server

If you are configuring MediaCentral Platform Services on a single server, the sharded Mongo configuration is automatically configured during the MCS installation process and no additional steps are required. In a single server configuration, sharded Mongo functions in standalone mode.

Configuring Sharded Mongo with an MCS Load-Balancing Node

If your environment consists of a Corosync cluster with three or more nodes, complete the following steps to create a sharded Mongo configuration with an arbiter located on a load-balancing node.

To configure sharded Mongo:

1. The sharded Mongo setup scripts rely heavily on correct hostname resolution and network availability. Before configuring Mongo, verify the following:
   a. Use the `hostname` command to verify the short host name of the node:

      `hostname`

      Repeat this command locally on each cluster node.

   b. Repeat the command using the "-f" switch to verify the node's fully qualified domain name (FQDN):

      `hostname -f`

      This command must return the host name with the full domain extension.

      Repeat this command locally on each cluster node.

   c. In addition to configuring all cluster nodes in the local hosts file, Avid recommends manually adding all cluster nodes to DNS. If the nodes have been added to DNS, use the nslookup command to verify that the DNS server responds with the correct information:

      `nslookup <node hostname>`

      Repeat the nslookup command for each cluster node (including the master), verifying that each node returns the correct information from DNS.

   d. When configuring a cluster, an "always on" pingable_ip address is used with the `setup-cluster` command. This IP address is used during the sharded Mongo setup and the process will fail if the address cannot be contacted. Verify that this address can be located on the network:

      `ping <IP address>`

   e. If your network crosses multiple switches, verify that the network ports required for sharded Mongo operation are open between the nodes.

      For more information, see the *Avid Networking Port Usage Guide* on the Avid Knowledge Base.

2. Verify that all cluster nodes are time synchronized.

   For detailed instructions, see "Configuring Date and Time Settings" on page 79.

3. Delete the default Mongo configuration by running the following script on each node:

   `mongo-clean-local`

   The script asks you to confirm that you wish to complete this action. Type **`y`** to continue.

   Complete this step on the Corosync master node, slave node, and all load-balancing nodes.

4. From the Corosync master node, run the configuration file creation script:

   `mongo-create-configuration`

If the script cannot connect to a node through SSH or the default password, you are asked to enter the root user password. If prompted, enter the root password for each node.

The script analyzes the current cluster configuration and prints its findings to the screen. This data is used by the final `mongo-playbook-setup` script, found later in this process, to create the sharded Mongo environment. Example output:

```
Collected configuration of online nodes:

ZONE_UUID                             ZONE_URL       ZONE_VERSION
00000000-0000-0000-0000-000000000000  192.168.10.51  2.9

NODE_UUID                             NODE_HOSTNAME  CLUSTER_ROLE  NODE_VERSION
00000000-0000-0000-0000-000000000000  wavd-mcs01     master        2.9
00000000-0000-0000-0000-000000000000  wavd-mcs02     slave         2.9
00000000-0000-0000-0000-000000000000  wavd-mcs03     balance       2.9
```

Review the following information to verify that the configuration data is correct:

- ZONE_UUID - Each zone in a multi-zone configuration is associated with a unique identifier (UUID). This section lists all zones found by the script. Systems that are not part of a multi-zone configuration list a single zone with a UUID of 00000000-0000-0000-0000-000000000000.
- ZONE_URL - In a single-zone environment, this is the IP address of the sharded Mongo management node.
- ZONE_VERSION - This is the version of MCS software running in each zone.
- NODE_UUID - This is a list of all nodes in the sharded Mongo configuration. If you have a single zone, a value of 00000000-0000-0000-0000-000000000000 is listed for all servers.
- NODE_HOSTNAME - This value represents the host name of the node.
- CLUSTER_ROLE - The script reports the role of each node as they are known in the Corosync cluster.
- NODE_VERSION - This is the version of MCS software running on each node.

Only online nodes are found by the script. If you have a Corosync node that is offline or in standby mode, it will not be listed. Before continuing, verify that all nodes are online.

5. Run the configuration file creation script again on the master node. This time, specify the “-c” switch to instruct the script to create the configuration files:

   `mongo-create-configuration -c`

6. The script updates the local Mongo hosts file which associates a node number with each cluster node. Additionally, multiple “`node<#>`” configuration files are created at `/opt/avid/installer/ansible/host_vars` (one for each Mongo node).

It is important to manually verify that the file is correct before continuing with the setup process. Review the file and verify its contents:

```
cat /opt/avid/installer/ansible/hosts
```

The following is an example of the file output:

```
#It's generated file from mongo-create-configuration script

[shards]
shard0 shard_tag=region-0

[mcs_servers]
node0 ansible_host=wavd-mcs01
node1 ansible_host=wavd-mcs02
node2 ansible_host=wavd-mcs03
```

Verify that each node is created with its short host name. If the wrong nodes have been populated, investigate and resolve the situation and run the script again.

Nodes are added to the configuration in the same order that they were added to the Corosync cluster. Node0 and node1 must be the master/slave pair for the cluster. Node2 must be a load-balancing node.

7. Prior to running the final setup script, you must first mount the Red Hat ISO image on the management node. The `mongo-playbook-setup` script referenced in this process requires that the ISO is mounted to the `/sysinstall` directory on the local node.

   a. Add the ISO to the system through one of the following methods:

      - Connect the MCS USB Installation Drive containing the Red Hat ISO to the server.
      - Burn the ISO to an optical disk and insert the disk on the server's optical drive.
      - Copy the ISO file to a directory on the local server such as `/media`.

Do not copy the ISO file directly to the /sysinstall directory.

   b. Mount the ISO to the `/sysinstall` directory:

      - If you have connected a USB drive, use the following command:

        ```
        mount /dev/<volume>/rhel-server-6.5-x86_64-dvd.iso /sysinstall
        ```

        In this command <*volume*> is the name associated with the USB drive. In a typical MCS configuration with a RAID5 array, this volume is `sdc1`.

      - If you have added an optical disk, use the following command:

        ```
        mount /dev/cdrom /sysinstall
        ```

      - If you have copied the ISO to a directory, use the following command:

        ```
        mount -o loop /<path>/rhel-server-6.5-x86_64-dvd.iso /sysinstall
        ```

        In this command <*path*> is the directory where you copied the ISO file.

8. From the sharded Mongo management node, run the final setup script:

   ```
   mongo-playbook-setup
   ```

   After a few moments, the script completes with a summary of the completed tasks:

   ```
   PLAY RECAP*****************************************************

   Node0    : ok=100   changed=20   unreachable=0   failed=0
   Node1    : ok=96    changed=25   unreachable=0   failed=0
   Node2    : ok=98    changed=28   unreachable=0   failed=0

   COMPLETED SUCCESSFULLY
   ```

Review the PLAY RECAP details and verify that there are no failed tasks. If there are no failed tasks, the sharded Mongo configuration has been successfully created.

You can further verify the configuration using the mongo-checker utility. For more information, see "Obtaining the Status of Sharded Mongo" on page 278.

If the script returns a "`COMPLETED WITH ERRORS!!!`" message, review the latest `mongo-playbook-setup_<`*`date`*`>.log` file for errors at: `/var/log/avid/ansible/`.

Configuring Sharded Mongo with a (non-MCS) Linux Arbiter

If your environment consists of a Corosync cluster with only two nodes (and no multi-zone), an arbiter must be added to the configuration. Avid supports configuring the arbiter on systems running either Red Hat Enterprise Linux (RHEL) v6.5 or CentOS v6.5. Since in this case the arbiter is not running on a MediaCentral server, the Mongo configuration files are not already present and must be added. This process requires that you have the Red Hat or CentOS ISO image available.

The non-MCS Linux arbiter can run any v6.x version of RHEL or CentOS. However, Avid recommends v6.5 to avoid any issues coping packages to the arbiter as described in this section.

Complete the following steps to create a sharded Mongo configuration with an arbiter located on a non-MCS Linux system. When completing any arbiter-specific steps, be sure that you are logged into Linux as a user with root level access.

To configure sharded Mongo:

1. Update the hosts file of the two Corosync nodes and the arbiter. The hosts file on each server must contain the IP address, hostname and FQDN of all three systems.

   For detailed instructions, see "Verifying the hosts File Contents" on page 74.

2. The sharded Mongo setup scripts rely heavily on correct hostname resolution and network availability. Before configuring Mongo, verify the following:

   a. Use the `hostname` command to verify the short host name of the node:

      `hostname`

      Repeat this command locally on each cluster node and the arbiter.

   b. Repeat the command using the "-f" switch to verify the node's fully qualified domain name (FQDN):

      `hostname -f`

      This command must return the host name with the full domain extension.

      Repeat this command locally on each cluster node and the arbiter.

   c. In addition to configuring all cluster nodes in the local hosts file, Avid recommends manually adding all cluster nodes to DNS. If the nodes have been added to DNS, use the nslookup command to verify that the DNS server responds with the correct information:

      `nslookup <`*`node hostname`*`>`

      Repeat the nslookup command for each cluster node (including the master) and the arbiter, verifying that each returns the correct information from DNS.

d. When configuring a cluster, an “always on” pingable_ip address is used with the `setup-cluster` command. This IP address is used during the sharded Mongo setup and the process will fail if the address cannot be contacted. Verify that this address can be located on the network:

   ```
   ping <IP address>
   ```

e. If your network crosses multiple switches, firewalls, or physical locations, verify that the network ports required for sharded Mongo operation are open between the nodes.

   For more information, see the *Avid Networking Port Usage Guide* on the Avid Knowledge Base.

3. Verify that the Linux arbiter is time synchronized with the cluster nodes.

   For detailed instructions, see “Configuring Date and Time Settings” on page 79.

4. Delete the default Mongo configuration on the Corosync master and slave nodes:

   ```
   mongo-clean-local
   ```

   The script asks you to confirm that you wish to complete this action. Type **y** to continue.

5. From the Corosync master node, run the configuration file creation script:

   ```
   mongo-create-configuration
   ```

If the script cannot connect to a node through SSH or the default password, you are asked to enter the root user password. If prompted, enter the root password for each node.

The script analyzes the current cluster configuration and prints its findings to the screen. This data is used by the final `mongo-playbook-setup` script, found later in this process, to create the sharded Mongo environment. Example output:

```
Collected configuration of online nodes:

ZONE_UUID                             ZONE_URL       ZONE_VERSION
00000000-0000-0000-0000-000000000000  192.168.10.51  2.9

NODE_UUID                             NODE_HOSTNAME  CLUSTER_ROLE  NODE_VERSION
00000000-0000-0000-0000-000000000000  wavd-mcs01     master        2.9
00000000-0000-0000-0000-000000000000  wavd-mcs02     slave         2.9
```

Review the following information to verify that the configuration data is correct:

- ZONE_UUID - Each zone in a multi-zone configuration is associated with a unique identifier (UUID). This section lists all zones found by the script. Systems that are not part of a multi-zone configuration list a single zone with a UUID of 00000000-0000-0000-0000-000000000000.
- ZONE_URL - In a single-zone environment, this is the IP address of the sharded Mongo management node.
- ZONE_VERSION - This is the version of MCS software running in each zone.
- NODE_UUID - This is a list of all nodes in the sharded Mongo configuration. If you have a single zone, a value of 00000000-0000-0000-0000-000000000000 is listed for all servers.
- NODE_HOSTNAME - This value represents the host name of the node.
- CLUSTER_ROLE - The script reports the role of each node as they are known in the Corosync cluster.
- NODE_VERSION - This is the version of MCS software running on each node.

Only online nodes are found by the script. If you have a Corosync node that is offline or in standby mode, it will not be listed. Before continuing, verify that all nodes are online.

6. Run the configuration file creation script again on the master node. This time, specify the "-c" switch to instruct the script to create the configuration files:

   `mongo-create-configuration -c`

   The script displays a message indicating that only 2 nodes are present in the cluster:

   ```
   ======================================================================

   Warning!!! You have one region and 2 nodes. In this configuration you need
   arbiter. Please prepare linux or windows host and add it to ansible
   configuration by running the script: '/opt/avid/bin/mongo-add-arbiter-
   configuration -n <hostname>'.
   Then run playbook for final installation: /opt/avid/bin/mongo-playbook-setup
   =====================================================================
   ```

   The script also provides guidance on how to resolve the issue. This is an expected warning for a two node configuration. Continue with the remaining steps in this process to complete the arbiter configuration.

   The script updates the local Mongo hosts file at `/opt/avid/installer/ansible` and creates multiple "`node<#>`" configuration files at `/opt/avid/installer/ansible/host_vars` (one for each Mongo node).

7. If your non-MCS Linux arbiter has SELinux (Security-Enhanced Linux) enabled, the "libselinux-python" package must be installed on the arbiter prior to running the script. This package is located on the Linux ISO.

   a. If you are unsure if SELinux is enabled, run the following command to verify the status:

      `cat /etc/sysconfig/selinux`

      The following is an example output of this file:

      ```
      # This file controls the state of SELinux on the system.
      # SELINUX= can take one of these three values:
      #     enforcing - SELinux security policy is enforced.
      #     permissive - SELinux prints warnings instead of enforcing.
      #     disabled - No SELinux policy is loaded.
      SELINUX=enforcing
      # SELINUXTYPE= can take one of these two values:
      #     targeted - Targeted processes are protected,
      #     mls - Multi Level Security protection.
      SELINUXTYPE=targeted
      ```

      By default, SELinix is enabled, as indicated above with the "enforcing" switch. On an MCS server, this setting is configured for "disabled".

      If desired, SELinux can be disabled by altering the SELINUX value from "enforcing" to "disabled" (without the quotes). If you alter this file, you must reboot the server to enable the change.

   b. Mount the Linux ISO through one of the following methods:

      - Connect the MCS USB Installation Drive containing the ISO to the server.
      - Burn the ISO to an optical disk and insert the disk on the server's optical drive.
      - Copy the ISO file to a directory on the local server such as `/media`.

Do not copy the ISO file directly to the /sysinstall directory.

c. Mount the ISO to the `/sysinstall` directory:

   - If you have connected a USB drive, use the following command:

     ```
     mount /dev/<volume>/<file-name> /sysinstall
     ```

     In this command *`<volume>`* is the name associated with the USB drive and *`<file-name>`* is the name of the operating system ISO file. In a typical MCS configuration with a RAID5 array, this volume is `sdc1`.

   - If you have added an optical disk, use the following command:

     ```
     mount /dev/cdrom /sysinstall
     ```

   - If you have copied the ISO to a directory, use the following command:

     ```
     mount -o loop /<path>/<file-name> /sysinstall
     ```

     In this command *`<path>`* is the directory where you copied the ISO file and *`<file-name>`* is the name of the operating system ISO file.

d. Issue the following command on the arbiter to install the package:

   ```
   yum install /sysinstall/Packages/libselinux-python*
   ```

   If this package is not installed, the `mongo-playbook-setup` script will fail with the following error:

   ```
   NO MORE HOSTS LEFT
   *************************************************************
       to retry, use: --limit @/opt/avid/installer/ansible/setup.retry
   *************************************************************
   COMPLETED WITH ERRORS!!!
   ```

   For more information on SELinux, see the following link: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security-Enhanced_Linux/chap-Security-Enhanced_Linux-Introduction.html

e. Once the package is installed, unmount the RHEL ISO from the arbiter:

   ```
   umount /sysinstall
   ```

8. To prepare to add an arbiter to the configuration, you must first mount the Red Hat ISO image on the management node. The `mongo-playbook-setup` script referenced in this process requires that the ISO is mounted to the `/sysinstall` directory on the local node.

   Refer to parts (b) and (c) of the previous step to mount the RHEL ISO on the sharded Mongo management node.

9. If the Linux firewall service is active on the Linux arbiter, the sharded Mongo management node might not be able to connect to it and the playbook script will fail. When installing MediaCentral Platform Services, the firewall is automatically disabled by the install script. When integrating with a non-MCS Linux server, you must disable the firewall service manually.

   a. Stop the firewall service, “iptables”, on the Linux arbiter:

      ```
      service iptables stop
      ```

   b. Configure the service to be disabled when Linux starts:

      ```
      chkconfig iptables off
      ```

   c. Verify that the service is disabled:

      ```
      chkconfig --list iptables
      ```

The output should be similar to the following:

```
iptables        0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

10. From the management node, run the "add-arbiter" script:

    ```
    mongo-add-arbiter-configuration --hostname=<hostname> --user=<user> --password=<pass>
    ```

    <*hostname*> is the short host name of the Linux arbiter.

    <*user*> should be a Linux user with root-level access. If this variable is not included in the command, the actual "root" user is used by default.

    <*pass*> is the password for the above user.

    The script is built for both Linux and Windows systems. It first checks for a connection to a Linux arbiter. If that fails, it attempts to connect to a Windows arbiter. For example:

    ```
    Public key for linux node wavd-mcsarbiter added successfully.
    COMPLETED SUCCESSFULLY
    Configuration added. For setup node, please run script: /opt/avid/bin/
    mongo-playbook-setup
    ```

    The script copies the SSH public key to the arbiter and verifies connection to the node. If successful, the arbiter is added to the `/opt/avid/installer/ansible/hosts` file, and a "`node2`" configuration file is created at: `/opt/avid/installer/ansible/host_vars`.

    For more information on this command, see "Using the mongo-add-arbiter-configuration Script" on page 290.

11. From the sharded Mongo management node, run the final setup script:

    ```
    mongo-playbook-setup
    ```

    The script completes a number of tasks, including the installation of the Mongo software packages on the arbiter. To be successful, network port 8085 must be open between the nodes to enable access to the `/opt/avid/Packages` and `/sysinstall` directories on the MCS server.

    After a few moments, the script completes with a summary of the completed tasks:

    ```
    PLAY RECAP****************************************************

    Node0    : ok=100   changed=20   unreachable=0   failed=0
    Node1    : ok=96    changed=25   unreachable=0   failed=0
    Node2    : ok=98    changed=28   unreachable=0   failed=0

    COMPLETED SUCCESSFULLY
    ```

    Review the PLAY RECAP details and verify that there are no failed tasks. If there are no failed tasks, the sharded Mongo configuration has been successfully created.

    You can further verify the configuration using the mongo-checker utility. For more information, see "Obtaining the Status of Sharded Mongo" on page 278.

    If the script returns a "`COMPLETED WITH ERRORS!!!`" message, review the latest `mongo-playbook-setup_<date>.log` file for errors at: `/var/log/avid/ansible/`.

Configuring Sharded Mongo with a Windows Arbiter

If your environment consists of a Corosync cluster with only two nodes, an arbiter must be added to the configuration. Avid supports configuring the arbiter on a system running Windows 7 (64 bit) SP1, Windows Server 2008 R2 (64 bit) SP1, or later.

Complete the following steps to create a sharded Mongo configuration with an arbiter located on a Windows system. When completing any of the Windows specific steps, be sure that you are logged into the Windows system as a user with administrator-level access.

⚠ **The "add-arbiter" and "mongo-playbook-setup" scripts in the following process have been known to fail in some situations where the Windows arbiter has been added to a domain and certain domain policies have been applied. If the script does not complete successfully, clean the sharded Mongo configuration on the MCS servers and refer to the process for "Configuring Sharded Mongo with a Windows Arbiter" in v2.7 of the *MediaCentral Platform Services Installation and Configuration Guide*. The v2.7 instructions provide a manual process for configuring the Windows arbiter.**

To configure sharded Mongo:

1. Update the local hosts file of the two Corosync nodes. The hosts file on each system must contain the IP address, hostname and FQDN of the two MCS servers and the Windows arbiter.

   For detailed instructions, see "Verifying the hosts File Contents" on page 74.

2. The sharded Mongo setup scripts rely heavily on correct hostname resolution and network availability. Before configuring Mongo, verify the following:

   a. Use the `hostname` command to verify the short host name of the node:

   ```
   hostname
   ```

   Repeat this command locally on each cluster node.

   b. Repeat the command using the "-f" switch to verify the node's fully qualified domain name (FQDN):

   ```
   hostname -f
   ```

   This command must return the host name with the full domain extension.

   Repeat this command locally on each cluster node.

   c. In addition to configuring all nodes in the local hosts file, Avid recommends manually adding all nodes to DNS. If the nodes have been added to DNS, use the nslookup command to verify that the DNS server responds with the correct information:

   ```
   nslookup <node hostname>
   ```

   Repeat the nslookup command for each cluster node (including the master) and the arbiter, verifying that each returns the correct information from DNS.

   d. When configuring a cluster, an "always on" pingable_ip address is used with the `setup-cluster` command. This IP address is used during the sharded Mongo setup and the process will fail if the address cannot be contacted. Verify that this address can be located on the network:

   ```
   ping <IP address>
   ```

e. If your network crosses multiple switches, firewalls, or physical locations, verify that the network ports required for sharded Mongo operation are open between the nodes.

   For more information, see the *Avid Networking Port Usage Guide* on the Avid Knowledge Base.

3. Verify that the Windows arbiter is time synchronized with the cluster nodes.

   For detailed instructions on configuring time-sync in a Windows environment, see Time Synchronization for Avid Interplay Systems on the Avid Knowledge Base.

4. Delete the default Mongo configuration on the master and slave nodes:

   ```
   mongo-clean-local
   ```

   The script asks you to confirm that you wish to complete this action. Type **y** to continue.

5. From the current Corosync master node, run the configuration file creation script:

   ```
   mongo-create-configuration
   ```

If the script cannot connect to a node through SSH or the default password, you are asked to enter the root user password. If prompted, enter the root password for each node.

The script analyzes the current cluster configuration and prints its findings to the screen. This data is used by the final `mongo-playbook-setup` script, found later in this process, to create the sharded Mongo environment. Example output:

```
Collected configuration of online nodes:

ZONE_UUID                              ZONE_URL       ZONE_VERSION
00000000-0000-0000-0000-000000000000   192.168.10.51  2.9

NODE_UUID                              NODE_HOSTNAME  CLUSTER_ROLE  NODE_VERSION
00000000-0000-0000-0000-000000000000   wavd-mcs01     master        2.9
00000000-0000-0000-0000-000000000000   wavd-mcs02     slave         2.9
```

Review the following information to verify that the configuration data is correct:

- ZONE_UUID - Each zone in a multi-zone configuration is associated with a unique identifier (UUID). This section lists all zones found by the script. Systems that are not part of a multi-zone configuration list a single zone with a UUID of 00000000-0000-0000-0000-000000000000.
- ZONE_URL - In a single-zone environment, this is the IP address of the sharded Mongo management node.
- ZONE_VERSION - This is the version of MCS software running in each zone.
- NODE_UUID - This is a list of all nodes in the sharded Mongo configuration. If you have a single zone, a value of 00000000-0000-0000-0000-000000000000 is listed for all servers.
- NODE_HOSTNAME - This value represents the host name of the node.
- CLUSTER_ROLE - The script reports the role of each node as they are known in the Corosync cluster.
- NODE_VERSION - This is the version of MCS software running on each node.

Only online nodes are found by the script. If you have a Corosync node that is offline or in standby mode, it will not be listed. Before continuing, verify that all nodes are online.

6. Run the configuration file creation script again on the master node. This time, specify the "-c" switch to instruct the script to create the configuration files:

   ```
   mongo-create-configuration -c
   ```

   The script displays a message indicating that only 2 nodes are present in the cluster:

   ```
   ====================================================================
   Warning!!! You have one region and 2 nodes. In this configuration you need
   arbiter. Please prepare linux or windows host and add it to ansible
   configuration by running the script: '/opt/avid/bin/mongo-add-arbiter-
   configuration -n <hostname>'.
   Then run playbook for final installation: /opt/avid/bin/mongo-playbook-setup
   ===================================================================
   ```

   The script also provides guidance on how to resolve the issue. This is an expected warning for a two node configuration. Continue with the remaining steps in this process to complete the arbiter configuration.

   The script updates the local Mongo hosts file at `/opt/avid/installer/ansible` and creates multiple "`node<#>`" configuration files at `/opt/avid/installer/ansible/host_vars` (one for each Mongo node).

7. The process to add a Windows arbiter requires the use of Windows PowerShell v3.0 or later. Prior to adding the arbiter, verify your version of PowerShell.

   a. Navigate to: Start > All Programs > Accessories > Windows PowerShell

   b. Right-click on Windows PowerShell and select "Run as administrator".

   c. Enter the following command in the PowerShell interface to verify the installed version of the software:

      ```
      $PSVersionTable
      ```

      PowerShell reports the version information for multiple components as shown in the following example:

      ```
      Name                           Value
      ----                           -----
      CLRVersion                     2.0.50727.5485
      BuildVersion                   6.1.7601.17514
      PSVersion                      2.0
      WSManStackVersion              2.0
      PSCompatibleVersions           {1.0, 2.0}
      SerializationVersion           1.1.0.1
      PSRemotingProtocolVersion      2.1
      ```

8. If you are already running PowerShell version 3.0 or later, skip to the next step in this process. If you are running PowerShell version 2.0, complete the following:

   a. PowerShell requires Microsoft .NET Framework. See the following two links to verify and if necessary, download the version of .NET Framework required for your system:

      https://msdn.microsoft.com/powershell/scripting/setup/windows-powershell-system-requirements

      https://www.microsoft.com/en-us/download/details.aspx?id=17851

      If .NET Framework is not installed prior to launching the PowerShell installer, the following error appears: "The update is not applicable to your computer."

b. Download an updated version of PowerShell for your operating system:

   https://www.microsoft.com/en-us/download/details.aspx?id=34595

   For more information on PowerShell and Windows version compatibility, see the following link: https://4sysops.com/archives/powershell-versions-and-their-windows-version/

c. Verify that the Windows Update service is running prior to launching the PowerShell installer. If it is not, the following error appears when launching the installer:

   "The service cannot be started, either because it is disabled or because it has no enabled devices associated with it."

d. If necessary, install or upgrade .NET Framework.

   Follow the on-screen instructions to install the software.

e. Use the installer you downloaded from the Microsoft website to upgrade PowerShell.

   Follow the on-screen instructions to install the software.

f. Verify that the installation was successful by verifying the PowerShell version. For example, a Windows 7 system installed with PowerShell v3.0 reports the following:

```
Name                           Value
----                           -----
PSVersion                      3.0
WSManStackVersion              3.0
SerializationVersion           1.1.0.1
CLRVersion                     4.0.30319.17929
BuildVersion                   6.2.9200.16398
PSCompatibleVersions           {1.0, 2.0, 3.0}
PSRemotingProtocolVersion      2.2
```

9. If your arbiter is running PowerShell v3.0, you must download and install a Microsoft hotfix to address an issue in PowerShell. Without this hotfix, the `mongo-playbook-setup` script will fail to configure the arbiter on the Windows system. You can download the hotfix from:

   https://support.microsoft.com/en-us/help/2842230

10. Verify that the Windows Firewall service is enabled and started. The "windows-ansible-prep" PowerShell script configures the firewall to allow communication between the arbiter and the other sharded Mongo nodes. If Windows Firewall is stopped, the following message is displayed when running the script: "An error occurred while attempting to contact the Windows Firewall service. Make sure that the service is running and try your request again."

    If your system normally operates with the Windows Firewall service disabled, temporarily enable and start the service. It can be disabled after the script has been run.

11. The MediaCentral_Services_<*version*>_Linux.zip installer package includes the "windows-ansible-prep.ps1" PowerShell script that is used to prepare the Windows arbiter.

    Copy this script to an easily accessible location on the Windows system such as: `c:\temp`.

12. Use Windows PowerShell to run the arbiter preparation script.

    a. Navigate to: Start > All Programs > Accessories > Windows PowerShell

       This location is correct for Windows 7. Location of the PowerShell application might vary depending on your version of Windows.

    b. Right-click on Windows PowerShell and select "Run as administrator".

c. Navigate to the directory containing the installation scripts:

```
cd <path>
```

Example:

```
cd c:\temp
```

d. Prior to running the script, you must alter the Execution Policy. Enter the following command:

```
Set-ExecutionPolicy RemoteSigned
```

The system replies with the following:

```
Execution Policy Change

The execution policy helps protect you from scripts that you do not
trust. Changing the execution policy might expose you to the security
risks described in the about_Execution_Policies help topic at http://
go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the
execution policy?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"):
```

Enter **Y** to enable the policy change.

e. Run the Avid provided script to prepare the Windows system to be configured as a sharded Mongo arbiter:

```
.\windows-ansible-prep.ps1
```

This script completes additional tasks on the Windows system to prepare it to be an arbiter.

The script completes with an “Ok” message.

13. To prepare to add an arbiter to the configuration, you must first mount the Red Hat ISO image on the management node. The `mongo-playbook-setup` script referenced in this process requires that the ISO is mounted to the `/sysinstall` directory on the local node.

    a. Add the ISO to the system through one of the following methods:

    - Connect the MCS USB Installation Drive containing the ISO to the server.
    - Burn the ISO to an optical disk and insert the disk on the server’s optical drive.
    - Copy the ISO file to a directory on the local server such as `/media`.

Do not copy the ISO file directly to the /sysinstall directory.

    b. Mount the ISO to the `/sysinstall` directory:

    - If you have connected a USB drive, use the following command:

      ```
      mount /dev/<volume>/rhel-server-6.5-x86_64-dvd.iso /sysinstall
      ```

      In this command <*volume*> is the name associated with the USB drive. In a typical MCS configuration with a RAID5 array, this volume is `sdc1`.

    - If you have added an optical disk, use the following command:

      ```
      mount /dev/cdrom /sysinstall
      ```

    - If you have copied the ISO to a directory, use the following command:

      ```
      mount -o loop /<path>/rhel-server-6.5-x86_64-dvd.iso /sysinstall
      ```

      In this command <*path*> is the directory where you copied the ISO file.

14. From the sharded Mongo management node, run the “add-arbiter” script:

    ```
    mongo-add-arbiter-configuration --hostname=<hostname> --user=<user> --password=<pass>
    ```

    `<hostname>` is the short host name of the Windows arbiter.

    `<user>` must be a local user account on the Windows system that is included in the “Administrators” user group. If this variable is not included in the command, the true “Administrator” account is used by default. Domain user accounts are not supported.

    `<pass>` is the password for the above user.

    The script is built for both Linux and Windows systems. It first checks for a connection to a Linux arbiter. If that fails, it attempts to connect to a Windows arbiter. For example:

    ```
    Can't get access to linux node wavd-mcsarbiter. Return code 1. Checking if
    it's windows...
    Connect to windows host wavd-mcsarbiter successfully.
    COMPLETED SUCCESSFULLY
    Configuration added. For setup node, please run script: /opt/avid/bin/
    mongo-playbook-setup
    ```

    The script verifies access to the arbiter and if successful, it adds the arbiter to the `/opt/avid/installer/ansible/hosts` file and creates a “`node2`” configuration file at: `/opt/avid/installer/ansible/host_vars`.

    The resulting `.../ansible/hosts` file should resemble the following:

    ```
    #It's generated file from mongo-create-configuration script

    [shards]
    shard0 shard_tag=region-0

    [mcs_servers]
    node0 ansible_host=wavd-mcs01
    node1 ansible_host=wavd-mcs02
    node2 ansible_host=wavd-mcsarbiter ansible_user='Administrator'
    ansible_password='Avid123' ansible_port=5986 ansible_connection=winrm
    ansible_winrm_server_cert_validation=ignore ansible_become=false
    ```

    For more information on this command, see “Using the mongo-add-arbiter-configuration Script” on page 290.

15. From the sharded Mongo management node, run the final setup script:

    ```
    mongo-playbook-setup
    ```

    After a few moments, the script completes with a summary of the completed tasks:

    ```
    PLAY RECAP*****************************************************

    Node0    : ok=100   changed=20   unreachable=0   failed=0
    Node1    : ok=96    changed=25   unreachable=0   failed=0
    Node2    : ok=98    changed=28   unreachable=0   failed=0

    COMPLETED SUCCESSFULLY
    ```

    Review the PLAY RECAP details and verify that there are no failed tasks. If there are no failed tasks, the sharded Mongo configuration has been successfully created.

    You can further verify the configuration using the mongo-checker utility. For more information, see “Obtaining the Status of Sharded Mongo” on page 278.

    If the script returns a “`COMPLETED WITH ERRORS!!!`” message, review the latest `mongo-playbook-setup_<date>.log` file for errors at: `/var/log/avid/ansible/`.

Configuring Sharded Mongo in a Multi-Zone Configuration

Multi-zone deployments are similar to local cluster deployments in that multiple nodes participate in the sharded configuration. The primary difference is the potential number of shards involved. As previously stated in the Overview, a sharded Mongo cluster is created across the zones.

Some versions of MediaCentral Platform Services are supported in a mixed multi-zone environment, where not all zones are running the same software version. Consult the *MediaCentral Platform Services ReadMe* or the *MediaCentral Platform Services Upgrade Guide* for specific version compatibility information.

Complete the following steps to create a multi-zone sharded Mongo installation. The “master node” in this process refers to the master node (sharded Mongo management node) of the master zone.

⚠ **Prior to completing this process, you must have a functional multi-zone configuration. For more information, see the chapter for configuring “Multi-Zone” on page 221.**

If you are creating a new multi-zone configuration and your environment consists of a two-node cluster that has already been configured for sharded Mongo, you must first remove the arbiter from the configuration before creating the sharded Mongo multi-zone environment. For the process to remove the arbiter, see “Working with Sharded Mongo” on page 277.

To configure sharded Mongo:

1. Update the hosts file on all nodes in all zones with the IP address, hostname and FQDN of any node that will host a Mongo shard. Shards exist on zones consisting of a single server or zones consisting of a Corosync master / slave set. Shards are not created on MCS load-balancing nodes.

   For detailed instructions, see “Verifying the hosts File Contents” on page 74.

2. The sharded Mongo setup scripts rely heavily on correct hostname resolution and network availability. Before configuring Mongo, verify the following:

   a. Use the `hostname` command to verify the short host name of the node:

   ```
   hostname
   ```

   Repeat this command locally on each server in the multi-zone configuration.

   b. Repeat the command using the “-f” switch to verify the node’s fully qualified domain name (FQDN):

   ```
   hostname -f
   ```

   This command must return the host name with the full domain extension.

   Repeat this command locally on each server in the multi-zone configuration.

   c. In addition to configuring the local hosts file on each MCS server, Avid recommends manually adding all servers to DNS. If the MCS servers have been added to DNS, use the nslookup command to verify that the DNS server responds with the correct information:

   ```
   nslookup <node hostname>
   ```

   Repeat the nslookup command for each server participating in the multi-zone configuration, verifying that each returns the correct information from DNS.

d. When configuring a cluster, an "always on" pingable_ip address is used with the `setup-cluster` command. This IP address is used during the sharded Mongo setup and the process will fail if the address cannot be contacted. If you are adding a zone in a clustered configuration, verify that this address can be located on the network:

```
ping <IP address>
```

Repeat this command for any cluster participating in the multi-zone configuration.

e. If your network crosses multiple switches, firewalls, or physical locations, verify that the network ports required for sharded Mongo operation are open between the nodes.

For more information, see the *Avid Networking Port Usage Guide* on the Avid Knowledge Base.

3. Verify that all nodes are time synchronized.

   For detailed instructions, see "Configuring Date and Time Settings" on page 79.

4. Delete the default Mongo configuration on **all** nodes in **all** zones that will take part in the sharded Mongo configuration, including the master node of the master zone:

   ```
   mongo-clean-local
   ```

   The script asks you to confirm that you wish to complete this action. Type **y** to continue.

5. From the master node of the master zone, run the following script to review the proposed sharded Mongo configuration:

   ```
   mongo-create-configuration
   ```

If the script cannot connect to a node through SSH with the default password, you are asked to enter the root user password. If prompted, enter the root password.

The script analyzes the current configuration of each zone and prints its findings to the screen. This data is used by the final `mongo-playbook-setup` script, found later in this process, to create the sharded Mongo environment. Example output:

```
Collected configuration of online nodes:

ZONE_UUID                             ZONE_URL       ZONE_VERSION
df613e50-074c-4aad-a8c3-8c21225503bc  192.168.10.51  2.9
612a0570-a694-4141-a5fb-5abc36f15d6d  news-mcs       2.9
54a3b6cb-7267-43bf-95e7-480cf27305c3  nyc-mcs        2.8

NODE_UUID                             NODE_HOSTNAME  CLUSTER_ROLE  NODE_VERSION
df613e50-074c-4aad-a8c3-8c21225503bc  wavd-mcs01     master        2.9
df613e50-074c-4aad-a8c3-8c21225503bc  wavd-mcs02     slave         2.9
df613e50-074c-4aad-a8c3-8c21225503bc  wavd-mcs03     balance       2.9
612a0570-a694-4141-a5fb-5abc36f15d6d  news-mcs       master        2.9
54a3b6cb-7267-43bf-95e7-480cf27305c3  nyc-mcs        master        2.8
```

Review the following information to verify that the configuration data is correct:

- ZONE_UUID - Each zone in a multi-zone configuration is associated with a unique identifier (UUID). This section lists all zones found by the script. Systems that are not part of a multi-zone configuration list a single zone with a UUID of 00000000-0000-0000-0000-000000000000. As this section focuses on multi-zone configurations, you should not see any zones listed with this UUID.

- ZONE_URL - In a multi-zone environment, this is the IP address or hostname of the node used to configure multi-zone environment in each zone.

- ZONE_VERSION - This is the version of MCS software running in each zone.

- NODE_UUID - This is a list of all nodes in the sharded Mongo configuration. In multi-zone configurations, each node reports its associated zone ID. All servers within a zone share the same UUID.
- NODE_HOSTNAME - This value represents the host name of the node.
- CLUSTER_ROLE - Zones consisting of a single server are listed as "master". If the zone consists of a cluster configuration, the nodes are listed as master, slave or balance (for load-balancing nodes).
- NODE_VERSION - This is the version of MCS software running on each node.

Only online nodes are found by the script. If you have a Corosync node that is offline or in standby mode, it will not be listed. Before continuing, verify that all nodes are online.

The example above indicates that this configuration consists of three zones. The first zone consists of a three-node cluster and the other two zones are single server configurations.

If the information is not correct, troubleshoot the issue before continuing.

6. From the master node of the master zone, run the configuration file creation script again. This time, specify the "-c" switch to instruct the script to create the configuration files:

   ```
   mongo-create-configuration -c
   ```

7. The script updates the local Mongo hosts file which associates a node number with the short host name of each server in the multi-zone environment. Additionally, multiple "`node<#>`" configuration files are created at `/opt/avid/installer/ansible/host_vars` (one for each Mongo node).

   It is important to manually verify that the file is correct before continuing with the setup process. Review the file and verify its contents:

   ```
   cat /opt/avid/installer/ansible/hosts
   ```

   The following is an example of the file output:

   ```
   #It's generated file from mongo-create-configuration script

   [shards]
   shard0 shard_tag=region-0
   shard1 shard_tag=region-1
   shard2 shard_tag=region-2

   [mcs_servers]
   node0 ansible_host=wavd-mcs01
   node1 ansible_host=wavd-mcs02
   node2 ansible_host=wavd-mcs03
   node3 ansible_host=news-mcs
   node4 ansible_host=nyc-mcs
   ```

   Verify that each node is created with its short host name. If the wrong nodes have been populated, resolve the situation and run the script again.

Verifying the hosts file is especially important for complex configurations as the script might populate the file with incorrect or non-optimal information.

8. Before configuring the sharded Mongo installation, you must first mount the Red Hat ISO image on the management node. The `mongo-playbook-setup` script referenced in this process requires that the ISO is mounted to the `/sysinstall` directory on the local node.

   a. Add the ISO to the system through one of the following methods:

      - Connect the MCS USB Installation Drive containing the Red Hat ISO to the server.
      - Burn the ISO to an optical disk and insert the disk on the server's optical drive.
      - Copy the ISO file to a directory on the local server such as `/media`.

Do not copy the ISO file directly to the /sysinstall directory.

   b. Mount the ISO to the `/sysinstall` directory:

      - If you have connected a USB drive, use the following command:

        ```
        mount /dev/<volume>/rhel-server-6.5-x86_64-dvd.iso /sysinstall
        ```

        In this command <*volume*> is the name associated with the USB drive. In a typical MCS configuration with a RAID5 array, this volume is `sdc1`.

      - If you have added an optical disk, use the following command:

        ```
        mount /dev/cdrom /sysinstall
        ```

      - If you have copied the ISO to a directory, use the following command:

        ```
        mount -o loop /<path>/rhel-server-6.5-x86_64-dvd.iso /sysinstall
        ```

        In this command <*path*> is the directory where you copied the ISO file.

9. From the sharded Mongo management node, run the final setup script:

   ```
   mongo-playbook-setup
   ```

   After a few moments, the script completes with a summary of the completed tasks:

   ```
   PLAY RECAP*************************************************

   Node0    : ok=100   changed=20   unreachable=0   failed=0
   Node1    : ok=96    changed=25   unreachable=0   failed=0
   Node2    : ok=98    changed=28   unreachable=0   failed=0
   Node3    : ok=98    changed=28   unreachable=0   failed=0
   Node4    : ok=93    changed=21   unreachable=0   failed=0

   COMPLETED SUCCESSFULLY
   ```

   Review the PLAY RECAP details and verify that there are no failed tasks. If there are no failed tasks, the sharded Mongo configuration has been successfully created.

   You can further verify the configuration using the mongo-checker utility. For more information, see "Obtaining the Status of Sharded Mongo" on page 278.

   If the script returns a "`COMPLETED WITH ERRORS!!!`" message, review the latest `mongo-playbook-setup_<date>.log` file for errors at: `/var/log/avid/ansible/`.

Adding a Zone to a Sharded Mongo Multi-Zone Environment

When working in a multi-zone configuration, it may not always be possible to upgrade all zones simultaneously. In that event, one or more zones might need to be upgraded at a later date and subsequently added to an existing sharded Mongo configuration. The following process details how to add a new zone to an existing sharded Mongo environment.

To configure sharded Mongo:

1. Install or upgrade the MCS servers in the new zone per the instructions in this guide or the *Avid MediaCentral Platform Services Upgrade Guide*.
2. Before reconfiguring sharded Mongo, the servers in the new zone should already be joined to the multi-zone configuration. For more information, see "Multi-Zone" on page 221.
3. Update the hosts file on all nodes in all zones with the IP address, hostname and FQDN of any node that will be joining the sharded Mongo configuration. The hosts file on the node or nodes in the new zone must contain the IP address and hostname information for all other sharded Mongo nodes.

   For detailed instructions, see "Verifying the hosts File Contents" on page 74.
4. The sharded Mongo setup scripts rely heavily on correct hostname resolution and network availability. Before configuring Mongo, verify the following:
   a. Connect locally to the first server that is being added to the multi-zone configuration and verify the hostname:

      ```
      hostname
      ```

      If you are adding a clustered system to the multi-zone configuration, repeat this command locally on each cluster node.

   b. Connect locally to the first server that is being added to the multi-zone configuration and repeat the command using the "-f" switch to verify the node's fully qualified domain name (FQDN):

      ```
      hostname -f
      ```

      This command must return the host name with the full domain extension.

      If you are adding a clustered system to the multi-zone configuration, repeat this command locally on each cluster node.

   c. In addition to configuring the local hosts file on each MCS server, Avid recommends manually adding all servers to DNS. If the MCS servers have been added to DNS, use the nslookup command to verify that the DNS server responds with the correct information:

      ```
      nslookup <node hostname>
      ```

      Repeat the nslookup command for each server being added to the multi-zone configuration, verifying that each returns the correct information from DNS.

   d. When configuring a cluster, an "always on" pingable_ip address is used with the `setup-cluster` command. This IP address is used during the sharded Mongo setup and the process will fail if the address cannot be contacted. If you are adding a clustered system to the multi-zone configuration, verify that the pingable_ip address of the new cluster can be located on the network:

      ```
      ping <IP address>
      ```

e. If your network crosses multiple switches, firewalls, or physical locations, verify that the network ports required for sharded Mongo operation are open between the nodes.

   For more information, see the *Avid Networking Port Usage Guide* on the Avid Knowledge Base.

5. Verify that all nodes are time synchronized.

   For detailed instructions, see "Configuring Date and Time Settings" on page 79.

6. Run the following command on all servers being added to the multi-zone configuration:

   ```
   mongo-clean-local
   ```

   The script asks you to confirm that you wish to complete this action. Type **y** to continue.

   If the zone being added to the configuration is a cluster, repeat the command on all cluster nodes in that zone.

The `mongo-clean-local` script deletes the default sharded Mongo configuration on the local node. DO NOT run the clean command on any server that is already a member of the sharded Mongo configuration.

7. Prior to making any changes to the configuration, review of the current ansible hosts file on the sharded Mongo management node:

   ```
   cat /opt/avid/installer/ansible/hosts
   ```

   The following is an example of the file output:

   ```
   #It's generated file from mongo-create-configuration script

   [shards]
   shard0 shard_tag=region-0
   shard1 shard_tag=region-1
   shard2 shard_tag=region-2

   [mcs_servers]
   node0 ansible_host=wavd-mcs01
   node1 ansible_host=wavd-mcs02
   node2 ansible_host=wavd-mcs03
   node3 ansible_host=news-mcs
   node4 ansible_host=nyc-mcs
   ```

   Take note of the current node order. When adding the new zone, it is very important that the numerical order (*node#*) of the existing nodes does not change.

8. From the master node of the master zone, run the following script to review the proposed sharded Mongo configuration:

   ```
   mongo-create-configuration
   ```

If the script cannot connect to a node through SSH with the default password, you are asked to enter the root user password. If prompted, enter the root password.

   The script analyzes the current configuration of each zone and prints its findings to the screen. This data is used by the final `mongo-playbook-setup` script, found later in this process, to create the sharded Mongo environment. Example output:

   ```
   Collected configuration of online nodes:

   ZONE_UUID                             ZONE_URL       ZONE_VERSION
   df613e50-074c-4aad-a8c3-8c21225503bc  192.168.10.51  2.9
   612a0570-a694-4141-a5fb-5abc36f15d6d  news-mcs       2.9
   ```

```
54a3b6cb-7267-43bf-95e7-480cf27305c3  nyc-mcs        2.8
777fh6a0-8456-22jk-76z2-512cvb7992ii  mynew-mcs      2.9

NODE_UUID                             NODE_HOSTNAME  CLUSTER_ROLE  NODE_VERSION
df613e50-074c-4aad-a8c3-8c21225503bc  wavd-mcs01     master        2.9
df613e50-074c-4aad-a8c3-8c21225503bc  wavd-mcs02     slave         2.9
df613e50-074c-4aad-a8c3-8c21225503bc  wavd-mcs03     balance       2.9
612a0570-a694-4141-a5fb-5abc36f15d6d  news-mcs       master        2.9
54a3b6cb-7267-43bf-95e7-480cf27305c3  nyc-mcs        master        2.8
777fh6a0-8456-22jk-76z2-512cvb7992ii  mynew-mcs      master        2.9
```

Review the following information to verify that the configuration data is correct:

- ZONE_UUID - Each zone in a multi-zone configuration is associated with a unique identifier (UUID). This section lists all zones found by the script. Systems that are not part of a multi-zone configuration list a single zone with a UUID of 00000000-0000-0000-0000-000000000000. As this section focuses on multi-zone configurations, you should not see any zones listed with this UUID.
- ZONE_URL - In a multi-zone environment, this is the IP address or hostname of the node used to configure multi-zone environment in each zone.
- ZONE_VERSION - This is the version of MCS software running in each zone.
- NODE_UUID - This is a list of all nodes in the sharded Mongo configuration. In multi-zone configurations, each node reports its associated zone ID. All servers within a zone share the same UUID.
- NODE_HOSTNAME - This value represents the host name of the node..
- CLUSTER_ROLE - Zones consisting of a single server are listed as “master”. If the zone consists of a cluster configuration, the nodes are listed as master, slave or balance (for load-balancing nodes).
- NODE_VERSION - This is the version of MCS software running on each node.

Only online nodes are found by the script. If you have a Corosync node that is offline or in standby mode, it will not be listed. Before continuing, verify that all nodes are online.

The example above indicates that this configuration consists of four zones. The first zone consists of a three-node cluster and other the three zones are single server configurations.

Verify that the server or servers from the newly added zone appear in the output.

If the information is not correct, troubleshoot the issue before continuing.

9. From the sharded Mongo management node, run the configuration file creation script again. This time, specify the “-c” switch to instruct the script to create the configuration files:

   `mongo-create-configuration -c`

   The script updates the local Mongo hosts file which associates a node number with the short host name of each server in the multi-zone environment. Additionally, multiple “node<#>” configuration files are created at /opt/avid/installer/ansible/host_vars (one for each Mongo node).

10. Review the contents of the ansible hosts file and verify that the expected changes have been made. It is important to verify that none of the original node#’s have been altered.

    `cat /opt/avid/installer/ansible/hosts`

    For more information about changes to the ansible hosts file, see “Using the mongo-create-configuration Script” on page 281.

11. To prepare to add an arbiter to the configuration, you must first mount the Red Hat ISO image on the management node. The `mongo-playbook-setup` script referenced in this process requires that the ISO is mounted to the `/sysinstall` directory on the local node.

    a. Add the ISO to the system through one of the following methods:

    - Connect the MCS USB Installation Drive containing the Red Hat ISO to the server.
    - Burn the ISO to an optical disk and insert the disk on the server's optical drive.
    - Copy the ISO file to a directory on the local server such as `/media`.

Do not copy the ISO file directly to the /sysinstall directory.

b. Mount the ISO to the `/sysinstall` directory:

- If you have connected a USB drive, use the following command:

  ```
  mount /dev/<volume>/rhel-server-6.5-x86_64-dvd.iso /sysinstall
  ```

  In this command `<volume>` is the name associated with the USB drive. In a typical MCS configuration with a RAID5 array, this volume is `sdc1`.

- If you have added an optical disk, use the following command:

  ```
  mount /dev/cdrom /sysinstall
  ```

- If you have copied the ISO to a directory, use the following command:

  ```
  mount -o loop /<path>/rhel-server-6.5-x86_64-dvd.iso /sysinstall
  ```

  In this command `<path>` is the directory where you copied the ISO file.

12. From the sharded Mongo management node, run the final setup script:

    ```
    mongo-playbook-setup
    ```

    The script will create a new shard with the proper shard tag, add new avid-iam shard replicas to the existing nodes, run sharded Mongo migration in "add region mode", and deploy the services on new node(s).

    After a few moments, the script completes with a summary of the completed tasks:

    ```
    PLAY RECAP**************************************************

    Node0    : ok=100   changed=20   unreachable=0   failed=0
    Node1    : ok=96    changed=25   unreachable=0   failed=0
    Node2    : ok=98    changed=28   unreachable=0   failed=0
    Node3    : ok=98    changed=28   unreachable=0   failed=0
    Node4    : ok=93    changed=21   unreachable=0   failed=0
    Node5    : ok=95    changed=21   unreachable=0   failed=0

    COMPLETED SUCCESSFULLY
    ```

    Review the PLAY RECAP details and verify that there are no failed tasks. If there are no failed tasks, the sharded Mongo configuration has been successfully created.

    You can further verify the configuration using the mongo-checker utility. For more information, see "Obtaining the Status of Sharded Mongo" on page 278.

    If the script returns a "`COMPLETED WITH ERRORS!!!`" message, review the latest `mongo-playbook-setup_<date>.log` file for errors at: `/var/log/avid/ansible/`.

7 Verifying the Installation

Chapter Overview

Step	Task	Time Est.
1	Testing the Basics	varies
	Covers a range of tests to verify your completed installation.	
2	Testing the Cluster Email Service	5 min
	Verifies that e-mails sent by the cluster will be delivered.	
3	Testing Cluster Fail-over	varies
	For configurations with a cluster, verifying fail-over is a crucial aspect of the installation and testing process.	
4	Verifying ACS Bus Functionality	5 min
	Verifies that the ACS bus and dependent services are communicating normally.	
5	Verifying the Status of RabbitMQ	5 min
	Verifies the status of the RabbitMQ messaging bus.	
6	Validating the FQDN for External Access	5 min
	Verifies that the MCS server(s) are accessible over the network.	
7	Backing up and Restoring the MCS System Settings and Database	10 min
	Provides a process to backup and restore the MCS settings.	

Testing the Basics

Because MCS provides workflows for many types of environments, testing steps may vary. Test the items that are applicable to your situation:

Testing MCS for MediaCentral and Media Composer Cloud:

- Can web-based clients sign into MediaCentral UX? Can they play media?
- Can mobile clients sign into MediaCentral UX? Can they play media?
- Can Media Composer Cloud clients upload/download media?
- Can users access and search the Interplay Production database?
- Can users access and search the iNEWS database?
- Can users create a sequence and Send To Playback?

Send To Playback is an excellent test as it simultaneously verifies connection to Avid shared storage, Interplay Production, MediaCentral Distribution Service, Interplay Production Services Engine, Interplay Transcode and potentially Interplay STP Encode and Interplay Transfer Engine.

- Can users initiate Delivery jobs to send media to a remote workgroup?
- Does the Messaging pane deliver messages between MediaCentral UX users? Does it deliver messages between MediaCentral UX and Media Composer?

Testing MCS for Interplay MAM:

- Proxy playback in the MAM Desktop
- Proxy playback in the MAM Cataloger Application
- MAM VideoAnalysis (video analysis of Proxy / Low-res material)
- MAM Connector: Proxy playback of MAM assets in MediaCentral UX

Testing the Cluster Email Service

The cluster automatically sends email notifications to the administrator email address. This requires that the Linux postfix email service is running on the master node and slave nodes. In this section you verify that the postfix service is operating as expected.

To test the cluster email service:

1. Verify the email service is running:

   ```
   service postfix status
   ```

   The system should respond with the following:

   ```
   master (pid XXXX) is running...
   ```

2. If the service is not running:

   a. Check the postfix service run-level configuration:

   ```
   chkconfig --list postfix
   ```

   The configuration should look like the following (run levels 2–5 on):

   ```
   postfix 0:off 1:off 2:on 3:on 4:on 5:on 6:off
   ```

   b. If run levels 2–5 are off, enable them with the following command:

   ```
   chkconfig postfix on
   ```

   c. Start the service:

   ```
   service postfix start
   ```

3. Complete steps 1 and 2 on the cluster slave node.
4. From the cluster master node, compose and send an email using the Linux `mail` command:

   ```
   mail -v <email address>
   ```

   The system responds by opening an email shell and prompting you for a subject line:

   ```
   Subject:
   ```

5. Enter a subject line and press Enter.

   The system responds by moving the cursor into the body of the email.

   Type a line or two of text, as desired.

If the Backspace key types "^H" rather than deleting, exit the email shell by typing Ctrl-C (twice). Next, type the following at the Linux command line, and try again (do not type the quotation marks: "stty erase ^H".

6. Type Ctrl+D to exit the email shell and send the email.

   The system responds with the following:

   ```
   Mail Delivery Status Report will be mailed to <root>.
   ```

7. Check the in-box of the addressee for the email.

For more information on using and configuring postfix, see the following link:

http://www.postfix.org/BASIC_CONFIGURATION_README.html

Testing Cluster Fail-over

If your configuration consists of a cluster, verifying the system's ability to fail-over from the Master node to the Slave node (and back again) is very important.

The cluster monitoring tool, crm_mon, provides a "live" view of the cluster and its associated resources. The tool can be launched in one of two ways:

- `crm_mon`
- `crm_mon -f`

Specifying the "-f" tells the tool to display the status of the cluster with fail-counts. Each time that a service fails, a node fail-count is retained by the system. Except for the AvidAll service, the default failure threshold for many of the services is two (2). Before testing the cluster, you will want to clear the fail-counts. If you do not, the cluster will fail-over automatically, and perhaps unexpectedly, when the threshold is reached.

To test cluster fail-over:

1. From a Windows machine, use an SSH utility such as PuTTY to open a remote session to any node in the cluster. Log in as the root user.
2. Launch the cluster monitoring tool, specifying the fail-count option:

   `crm_mon -f`

   This returns the status of all cluster-related services on all nodes, with output similar to the following thee node (wavd-mcs01, wavd-mcs02 & wavd-mcs03) example:

```
Last updated: Tue Jun  5 16:10:18 2016
Last change: Tue Jun  5 16:08:09 2016
Current DC: wavd-mcs03 - partition with quorum
3 Nodes and 35 Resources configured

Online: [ wavd-mcs01 wavd-mcs02 wavd-mcs03 ]

 Clone Set: AvidConnectivityMonEverywhere [AvidConnectivityMon]
     Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03 ]
AvidClusterMon  (lsb:avid-monitor):     Started wavd-mcs01
MongoDB (lsb:mongod):   Started wavd-mcs01
Redis   (ocf::avid:redis):      Started wavd-mcs01
 Resource Group: postgres
     postgres_fs   (ocf::heartbeat:Filesystem):    Started wavd-mcs01
     AvidClusterIP (ocf::heartbeat:IPaddr2):       Started wavd-mcs01
     pgsqlDB    (ocf::avid:pgsql_Avid): Started wavd-mcs01
 Master/Slave Set: ms_drbd_postgres [drbd_postgres]
     Masters: [ wavd-mcs01 ]
     Slaves: [ wavd-mcs02 ]
 Clone Set: AvidAllEverywhere [AvidAll]
     Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03 ]
AvidIPC (lsb:avid-interplay-central):   Started wavd-mcs01
AvidUpstream    (lsb:avid-upstream):    Started wavd-mcs01
 Clone Set: AvidIamEverywhere [AvidIam]
     Started: [ wavd-mcs01 wavd-mcs02 ]
 Clone Set: AvidAssetEverywhere [AvidAsset]
     Started: [ wavd-mcs01 wavd-mcs02 ]
 Clone Set: AvidAssetGcEverywhere [AvidAssetGc]
     Started: [ wavd-mcs01 wavd-mcs02 ]
AvidUMS (lsb:avid-ums): Started wavd-mcs01
AvidUSS (lsb:avid-uss): Started wavd-mcs01
AvidACS (lsb:avid-acs-ctrl-core):       Started wavd-mcs01
AvidServiceManager (lsb:avid-acs-service-manager): Started wavd-mcs01
 Clone Set: AvidGatewayEverywhere [AvidGateway]
     Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03 ]
 Clone Set: AvidICPSEverywhere [AvidICPS]
     Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03 ]
 Clone Set: AvidNginxEverywhere [AvidNginx]
     Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03 ]

Migration summary:
* Node wavd-mcs02:
* Node wavd-mcs01:
* Node wavd-mcs03:
```

The master node is always the owner of the AvidClusterIP resource. It also manages multiple other resources such as:

- pgsqlDB (PostgreSQL database)
- AvidUMS (Avid User Management Service)
- And more...

The prefix lsb shown in the Cluster Resource Monitor indicates the named service conforms to the Linux Standard Base project, meaning these services support standard Linux commands for scripts (e.g. start, stop, restart).

3. Check the tool for fail-counts. If failures exist, they will be displayed per node in the "Migration summary" area at the bottom of the window. Example:

```
Migration summary:
* Node wavd-mcs01:
  AvidIPC: migration-threshold=2 fail-count=1
  AvidAll:0: migration-threshold=1000000 fail-count=58

* Node wavd-mcs02:
  AvidAll:2: migration-threshold=1000000 fail-count=77

Failed actions:  AvidAll_monitor_25000 on wavd-mcs01 'not running' (7):
call=574, status=complete, last-rc-change='Wed Jun 25 13:13:15 2014,
queued=0ms, exec=0ms
```

Make sure your SSH window is large enough (vertically) to see the fail-counts.

4. If failures exist, they need to be cleared before testing fail-over:

```
crm resource cleanup <rsc> [<node>]
```

- `<rsc>` is the resource name of interest: AvidIPC, AvidUMS, AvidACS, etc.
- `<node>` (optional) is the node of interest. Omitting the node cleans up the resource on all nodes.

Some resources can be addressed individually or as part of a group. For instance, the postgres resource group consists of three resources: postgres_fs, AvidClusterIP and pgsqlDB.

Other resources must be cleared using the "Everywhere" version of the resource. For example, to reset the fail-count for AvidAll resource, issue the following command:

```
crm resource cleanup AvidAllEverywhere
```

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the group name for the resource (the "everywhere" form).

Once all failures have been cleared, the Migration summary should look like the following:

```
Migration summary:
* Node wavd-mcs01:
* Node wavd-mcs02:
```

5. Once the tool is free of failures, identify and make note of the Master node.

6. From a Windows machine, use an SSH utility such as PuTTY to open a second remote session to another node in the cluster. Make sure to specify a different node than the one opened in the previous SSH session. Log in as the root user.

7. Put the Master node into standby:

   ```
   crm node standby <hostname>
   ```

   Replace <*hostname*> with the hostname of the Master node (e.g. wavd-mcs01).

8. Observe the fail-over in the crm_mon utility within the other terminal session. The former Master node will be put into standby. The former Slave node will become the new master and services will begin to come online under that new Master node.

During the fail-over process, any active MediaCentral clients will receive a message indicating the need to sign back in.

9. If fail counts were added to the monitoring tool, clear them with the `crm resource cleanup` command.

10. Perform some basic testing of the system such as logging into MediaCentral UX, verifying access to the associated databases (Interplay, iNEWS), verify playback, etc.

11. Bring the standby node back online:

    ```
    crm node online <hostname>
    ```

    Replace <*hostname*> with the hostname of the offline node (e.g. wavd-mcs01).

    Observe in the crm_mon window as the offline node is brought back up and rejoins the cluster. This node will now take on the role of the Slave node.

12. If fail counts were added to the monitoring tool, clear them with the `crm resource cleanup` command.

13. Repeat the process to test fail-over in the opposite direction. Remember to clear any fail counts at the end of the process and verify basic functionality.

Verifying ACS Bus Functionality

The Avid Common Services bus (“the bus”) provides essential bus services needed for the overall platform to work. Numerous services depend upon it, and will not start — or will throw serious errors — if the bus is not running. You can easily verify ACS bus functionality using the acs-query command. On a master node, this tests the ACS bus directly. Although the ACS bus operates on the master and slave nodes only, by running acs-query on a non-master node you can validate network and node-to-node bus connectivity.

To verify the ACS bus is functioning correctly:

1. Query the ACS bus database using the acs-query command with using the --path option:

   ```
   acs-query --path=serviceType
   ```

2. Review the output. It should report information similar to the following:

   ```
   "avid.acs.registy"
   ```

   This indicates that RabbitMQ, MongoDB and PostgreSQL are all running and are reachable by the ACS bus (since no errors are present). It also indicates the “avid.acs.registry” bus service is available.

Verifying the Status of RabbitMQ

RabbitMQ is a messaging bus used by the top-level MCS services on each node to communicate with each other. It maintains its own cluster functionality independent of the Corosync cluster. Special care must be taken when rebooting or shutting down MCS servers as incorrect procedures could break the RabbitMQ cluster.

For more information on RabbitMQ, see the *MediaCentral Platform Services Concepts and Clustering Guide*.

To verify the RabbitMQ service status:

1. The following command checks the status of the rabbitmq-server service:

   ```
   service rabbitmq-server status
   ```

   The command will return a detailed string of data regarding the service. Example (partial only):

   ```
   [root@wavd-mcs01 ~]# service rabbitmq-server status
   Status of node 'rabbit@wavd-mcs01' ...
   [{pid,2064},
    {running_applications,
        [{rabbitmq_federation_management,"RabbitMQ Federation Management",
             "3.3.5"},
         {rabbitmq_management,"RabbitMQ Management Console","3.3.5"},
   ```

2. Review the output of the command and verify there are no obvious error messages such as “service is dead but pid (xxxxx) is running”.
3. Repeat the command on each cluster node.

To verify that RabbitMQ cluster status:

1. Request the status of the messaging bus using the rabbitmqctl command:

   ```
   rabbitmqctl cluster_status
   ```

   Example output for a two node cluster:

   ```
   [root@wavd-mcs01 ~]# rabbitmqctl cluster_status
   Cluster status of node 'rabbit@wavd-mcs01' ...
   [{nodes,[{disc,['rabbit@wavd-mcs01','rabbit@wavd-mcs02']}]},
   {running_nodes,['rabbit@wavd-mcs01','rabbit@wavd-mcs02']},
   {cluster_name,<<"rabbit@wavd-mcs01.wavd.com">>},
   {partitions,[]}]
   ...done.
   ```

2. Review the output of the command.

   The command should return information about each of the RabbitMQ cluster nodes. All available nodes should appear on both the “nodes” and “running_nodes” lines.

   If you do not see results similar to those listed in the example above or if you need additional information on RabbitMQ, including troubleshooting assistance, see:

   http://avid.force.com/pkb/articles/en_US/troubleshooting/RabbitMQ-cluster-troubleshooting

3. Repeat the command on each cluster node.

   Verify that each node reports the same information about the RabbitMQ cluster (all nodes are known and running).

Validating the FQDN for External Access

It is vital that the fully qualified domain names (FQDN) for all MCS servers are resolvable by the domain name server (DNS) tasked with doing so. This is particularly important when MediaCentral Platform Services will be accessed from the MediaCentral UX mobile application (iPad, iPhone or Android device) or when connecting from outside the corporate firewall through Network Address Translation (NAT). In such cases, review the FQDN returned by the XLB load balancer. Ensure that the network administrator has assigned the FQDN a unique public IP address.

Currently, connecting to MediaCentral UX through NAT is supported only for single-server configurations, not MCS cluster configurations.

To validate the FQDN of the MCS Servers:

1. Launch a web browser on your client(s) of interest. This could be:
   - An iPad, iPhone or Android device
   - A client outside of the corporate firewall through a VPN or NAT connection
   - A client within the corporate firewall
2. Enter the following URL into the address bar:

   http://<*FQDN*>/api/xlb/nodes/less/?service=xmd

   Where <*FQDN*> is the fully qualified domain name of the MCS server. In a cluster configuration, enter the FQDN of the cluster (virtual cluster hostname). For example:

   http://**wavd-mcs.wavd.com**/api/xlb/nodes/less/?service=xmd

   The system returns a string similar to the following (line breaks added for clarity):

   ```
   {"status":"ok","data":
   {"xlb_service_ip":"10.XXX.XXX.XX",
   "xlb_service_port":5000,
   "xlb_node_ip":"10.XXX.XXX.XX/32",
   "xlb_node_name":"wavd-mcs01",
   "xlb_node_full_name":"wavd-mcs01.subdomain.domain.net"}}
   ```

   Note the following data of interest:

Item	Description
xlb_node_ip	The IP address of the node assigned to you for the current session. In a cluster configuration, this will be one of the cluster nodes.
xlb_node_name	The host name of the node assigned to you for the current session. In a cluster configuration, this will be one of the cluster nodes.
xlb_node_full_name	The FQDN of the assigned node. If connecting to MediaCentral UX from outside the corporate firewall through NAT, this domain name must resolve to an external (public) IP address.

An example of a failed connection from the Safari browser on an iOS device appears as follows: "Safari cannot open the page because the server cannot be found."

3. Verify the output of the command.

   For a Single Server:

In a single server configuration, the “xlb_node_full_name” should match the FQDN name entered in the Server field of the MediaCentral System Setting (System Settings > MCPS > Player > Server).

For a Cluster:

In a cluster configuration, the domain extension (e.g. wavd.com) displayed in “xlb_node_full_name” should match the domain extension used in the Server field of the MediaCentral System Setting (System Settings > MCPS > Player > Server).

In this case you are only matching the domain extension because the Server field in the MediaCentral System Settings specified the cluster name and not an individual node.

The “xlb_node_full_name” will not return the cluster FQDN, but will instead return one of the cluster’s individual node names. The returned node name is based on whichever node is most available to respond for the current session.

Refreshing the web page may return a different node name. This is normal.

If the output does not match, you might be able to sign into MediaCentral UX on a remote client, but playback might not function.

If MediaCentral will be accessed from outside the corporate firewall through NAT, ensure that this server is accessible. In particular, ensure the FQDN returned by the query is associated with a public address.

Troubleshooting:

If you are not getting the results you expect, work with your on-site IT Department to verify that your DNS includes forward and reverse entries for each MCS server and an entry for the virtual cluster hostname and IP. Make sure there are no duplicate entries that contain incorrect information (e.g. an invalid IP address).

If you are still unsuccessful and you are not using NAT, an alternative option exists. MCS v2.0.2 added a feature for altering the “application.properties” file to instruct the MCS servers to return an IP address during the load-balancing handshake instead of a hostname. Refer to “Modifying application.properties” on page 252 for instructions.

This process is not supported for single-server systems using NAT.

Once the application.properties file has been updated, repeat the FQDN validation process.

Backing up and Restoring the MCS System Settings and Database

Now that the MediaCentral system is fully configured, consider this an excellent moment to back up the system settings. In the event you need to re-image the server, or upgrade MCS, having a backup of the settings is invaluable.

The `system-backup` script provided on the MCS Installation USB Drive backs up important files and directories, including NIC card settings, DNS settings, and so on. In addition, the script calls the *avid-db* command, which dumps and backs up the contents of the MCS database. The MCS database contains ACS (Avid Common Services, “the bus”), UMS (User Management Services) and MCPS (MediaCentral Playback Services) data. It collects all this information and backs it up to the USB drive itself. If installed, the avid-db command also creates a backup of the Customizable Logger database stored in MongoDB.

In a cluster, the MCS database is replicated across the master and slave node, but it is only mounted on the master. Thus, the MCS database is only available for dumping and backup on the master node.

If you are creating back-ups for multiple cluster nodes, rename the backup file for each node before proceeding to the next node. If you do not rename the backup file obtained from the master node, it will be overwritten by the backup from a non-master node and the contents of the MCS database will be lost (including user information).

The following table lists the files and directories backed up and restored by the system-backup script. The table lists files as they are found in the `ics_setup_files.tar` backup file:

Directory/File	Description
/etc/bucardorc	Bucardo configuration file used for database replication in a cluster
/etc/collectd.conf	Configuration file for the collectd service
/etc/localtime	Time zone info
/etc/ntp.conf	Network Time Protocol config file
/etc/redis.conf	Configuration file for the redis service
/etc/resolv.conf	/etc/resolv.confDNS config file
/etc/sudoers	List of users with sudo privileges
/etc/collectd.d/	Configuration files for the collectd service
/etc/corosync/corosync.conf	Corosync config file (cluster only)
/etc/cron.d/ntpd	The cron job that automates synchronization of the system clock.
/etc/drbd.d/r0.res	DRDB config file (cluster only)
/etc/elasticsearch/ /etc/elasticsearch-tribe/	Settings related to Media Index
/etc/pgpool-II/	Settings related to Multi-Zone configs
/etc/rsyslog.d/	Configuration file pertaining to the ICPS service
/etc/security/	
/etc/snmp/	Simple Network Management Protocol (network monitor)
/etc/sudoers.d/	List of users with sudo privileges
/etc/sysconfig/	Network settings and more
/etc/udev/rules.d/70-persistent-net.rules	NIC card settings
/opt/avid/etc/avid/avid-interplay-central/ssl/jetty.keystore	SSL private key file used with MCS 2.4 and earlier
/opt/avid/etc/pki/certs/site.crt /opt/avid/etc/pki/private/site.key	SSL Certificate (site.crt) and private key (site.key) files used with MCS 2.5 and later.
/opt/avid/etc/avid/avid-interplay-central/config/application.properties	Contains customized options for MCS.

Directory/File	Description
/root/	Filesystem settings originally obtained from /etc/fstab
/usr/maxt/maxedit/etc/*	Maxedit settings (used by ICPS)
/usr/maxt/maxedit/share/MPEGPresets/MPEG2TS.mpegpreset	Defines encoding for iOS playback
/var/lib/avid/db/dumps var/lib/avid/db/mongodump/*	ICS/MCS database (ACS, UMS and ICPS data). This includes user information.
RHEL user names and passwords	***** Not backed up. *****

RHEL user names and passwords (such as the root user) are not backed up or restored by the system-backup script. After the upgrade, logging in as "root" requires the default password (Avid123).

To back up the system settings and MCS database:

1. Mount the original MCS Installation USB drive that contains the system-backup script.

   For detailed instructions, see "Copying Software Using a USB Drive" on page 239.

2. Change to the mount point. For example:

   ```
   cd /media/usb
   ```

3. Back up the MCS settings and database using the backup script:

   ```
   ./system-backup.sh -b
   ```

When backing up the master node in a cluster, it must not be in standby mode. When backing up other nodes, they can be in standby.

   A backup file is written to the USB drive:

   ```
   /media/usb/sys-backup/ics_setup_files.tar.gz
   ```

   Since the system-backup script also calls the avid-db command, a backup of the MCS database is also written to the following directory (on the MCS server):

   ```
   /var/lib/avid/db/dumps
   ```

   The backup file on the server has a name has the following form:

   ```
   ALL-YYYYMMDD_HHMMSSZ.sql.gz.cr
   ```

The time stamp appended to the file name uses the Universal Time Code (UTC), not the local time.

   The following message indicates success:

   ```
   Backup setup successful!
   ```

4. Rename the backup file on the USB drive using the Linux `mv` command. For example:

   ```
   mv sys-backup sys-backup-<nodename>
   ```

   The above command renames the directory containing the backup file just created. The backup file itself (`ics_setup_files.tar.gz`) remains unchanged inside the directory.

Renaming the backup file is particularly important if you are backing up multiple nodes in a cluster. Only the master node backup contains a complete set of backup information. If you do not rename the master node backup file, it will be overwritten by the backup from a non-master node.

5. Unmount the USB drive.

   For detailed instructions, see “Copying Software Using a USB Drive” on page 239.

6. If you have a cluster, repeat the process on each node.

To restore the system settings and MCS database:

In the event that you need to restore system settings to the MCS servers, the following process is provided. This step should not be completed when testing the system.

1. Mount the original MCS Installation USB drive that contains the system-backup script.

   For detailed instructions, see “Copying Software Using a USB Drive” on page 239.

2. Change to the mount point. For example:

   ```
   cd /media/usb
   ```

3. If you renamed the backup file, restore it to the original name:

   ```
   mv sys-backup-<nodename> sys-backup
   ```

4. Restore the MCS settings and database using the backup script:

   ```
   ./system-backup.sh -r
   ```

   You are asked to confirm the restoration of the MCS database:

   ```
   Would you like to restore the database now? (y/n)
   ```

5. Type “**y**” (without the quotes) to confirm the action.

   You are asked to confirm the shutting down of the Avid services:

   ```
   All Avid services will be shut down before performing a database restore
   operation.
   ```

   ```
   Would you like to continue? [yes/no]
   ```

6. Type “**yes**” (spelled out in full, without the quotes) to confirm the action.

Be careful when typing your response to this question. Typing anything other than “yes” results in the script exiting without restoring the MCS database. Other items are restored, but not the MCS database.

   Services are shut down, the MCS database is restored, and services are restarted.

   The MCS database service is stopped, and you are prompted to restore the database.

   The following message indicates success:

   ```
   Restoration done!
   Your old fstab settings were saved in /root/fstab
   Please remove the USB key and reboot the server.
   ```

The filesystem table (fstab) file contains information to automate mounting volumes at boot time. It is not restored automatically.

7. Once the settings are restored, unmount and remove the USB drive.

   For detailed instructions, see “Copying Software Using a USB Drive” on page 239.

8. If you have a cluster, repeat the process on each node.

8 Closed Captioning Service

Chapter Overview

The purpose of this chapter is to guide you through the installation of the Closed Captioning Service (CCS) introduced with MediaCentral Platform Services v2.3.

The following table describes the topics that are covered in this chapter:

Step	Task	Time Est.
1	Preparing the Software Package	5 min
	Process for copying and unzipping the CC installer.	
2	Preparing the Software Package	5 min
	Process for installing the CC Service on a single MCS server.	
3	Installing the Closed Captioning Service in a Cluster	15 min
	Process for installing the CC Service on an MCS cluster.	

The Closed Captioning Service adds new functionality to MediaCentral UX in the form of a Closed Captioning pane. Broadcasters face increased pressure to include closed captioning information in their content due to government regulations. Through this pane, editors can review, edit, and repackage closed captioning data contained in Sequences. Closed captioning data can also be imported from file and exported to file from within MediaCentral UX.

The Closed Captioning Service installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and sign off during the installation or upgrade procedures.

Ensure that the *Virtual Host Name* field within the Storage Locations section of the "Playback Service Settings" on page 100 is entered in all lower case. If it is not, you may experience errors similar to the following:

```
"Error while calling action: Error while extracting CC data from Interplay
data: CC Conversion Service: Failed to read filepath=<path>"
```

The process for upgrading an existing installation and performing a new installation of the Closed Captioning Service are the same. The upgrade process simply overwrites the appropriate files.

MediaCentral Platform Services v2.3 through v2.6 required the Closed Captioning Service to be installed on all cluster nodes. If you are upgrading from an older version of the software, follow the process for "Uninstalling the Closed Captioning Service" on page 171 to uninstall the service on the load-balancing nodes.

Preparing the Software Package

Before you can start the installation, you must obtain the Closed Captioning Service software and copy it to your MediaCentral server. If you have a cluster configuration, complete steps below on the master and slave nodes only.

To prepare the software package:

1. Ensure that you have obtained and copied the Closed Captioning Service software to the MCS server(s). If you have not completed these tasks, see "Obtaining the Software" on page 21 and "Copying Software to the MCS Server" on page 238 for instructions.
2. Navigate to the directory where the installer has been copied. Example:

   ```
   cd /media/installers
   ```

3. If necessary, unzip the CC Service installer:

   ```
   unzip MediaCentral_ClosedCaptioning_Service_<x.x.x>_Linux.zip
   ```

4. Navigate to the newly created directory:

   ```
   cd MediaCentral_ClosedCaptioning_Service_<x.x.x>_<build>_Linux
   ```

Installing the Closed Captioning Service on a Single Server

The following instructions apply to installing the Closed Captioning Service on a single-server installation. If you are in a clustered configuration, refer to "Installing the Closed Captioning Service in a Cluster" on page 168.

To install the Closed Captioning Service:

1. If you have not already done so, navigate to the directory containing the installation script:

   ```
   cd /<path>
   ```

2. Run the CC Service installation script:

   ```
   ./install.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   The end of the CCS installation process should indicate a successful installation:

   ```
   Complete!
   Restarting avid-interplay-central on standalone node
   avid-ccc is not running                            [  OK  ]
   avid-ccc [1] starting...                           [  OK  ]
   avid-ccc [2] starting...                           [  OK  ]
   avid-ccc [3] starting...                           [  OK  ]
   avid-ccc [4] starting...                           [  OK  ]
   avid-ccc [5] starting...                           [  OK  ]
   Avid Interplay Central process has been started.
   Wait for Interplay Central web interface...
   Avid Interplay Central has been started successfully (31 seconds)
   ```

3. Verify the success of the installation using the Linux rpm command:

   ```
   rpm -qa | grep avid-ccc
   ```

   The output should include the following lines:

   ```
   avid-ccc-anc-<version>.x86_64
   avid-ccc-cluster-config-<version>.x86_64
   avid-ccc-<version>.x86_64
   ```

Installing the Closed Captioning Service in a Cluster

In a cluster deployment, the Closed Captioning Service is installed on the master and slave nodes only. A new AvidCCC resource is added to the cluster during installation. This resource is active on the master node and migrates to the slave node during a fail-over.

The cluster installation process involves the following steps:

- Preparing the Software Package
- Verifying Prerequisites
- Identifying the Master, Slave and Load-Balancing Nodes
- Taking the Cluster Offline
- Installing the Closed Captioning Service Software
- Bringing the Cluster Online
- Checking on the Cluster Status

If you are in a clustered configuration, refer to “Installing the Closed Captioning Service on a Single Server” on page 167.

Verifying Prerequisites

Prior to installing the Closed Captioning Service, verify the following:

- MCS is installed and configured on all servers in the cluster.
- All cluster resources should be online and free of errors.

  Use “`crm_mon -f`” to verify the cluster status.

Identifying the Master, Slave and Load-Balancing Nodes

There are three types of nodes in a cluster: master, slave, and load-balancing. The master “owns” multiple resources such as the cluster IP address. The slave assumes the role of master in the event of a fail-over. Additional nodes play a load-balancing role, but can never take on the role of master.

To identify the master, slave, and load-balancing nodes:

1. Verify the current role of each node by logging in to any machine in the cluster as the root user and typing:

   ```
   crm_mon
   ```

2. To identify the master and slave nodes, look for the line containing “Master/Slave Set”.

   For example:

   ```
   Master/Slave Set: ms_drbd_postgres [drbd_postgres]
   Masters: [ wavd-mcs01 ]
   Slaves: [ wavd-mcs02 ]
   ```

   In this example, the master node is wavd-mcs01 and the slave node is wavd-mcs02.

3. To identify the load-balancing nodes, look for the line containing “Clone Set”:

   ```
   Clone Set: AvidAllEverywhere [AvidAll]
   Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03]
   ```

   In this example, the load-balancing node is wavd-mcs03.

4. Exit crm_mon by pressing CTRL-C on the keyboard.

Taking the Cluster Offline

Prior to installing the Closed Captioning Service, all nodes must be taken offline. To avoid accidental cluster fail-over, make sure to follow the order represented below.

To take the cluster offline:

1. Begin taking the cluster offline by putting the load-balancing nodes into standby mode:

   ```
   crm node standby <node name>
   ```

2. Next, put the slave node into standby mode:

   ```
   crm node standby <node name>
   ```

3. Finally, put the master node into standby mode:

   ```
   crm node standby <node name>
   ```

Installing the Closed Captioning Service Software

Complete the following process on the cluster master and slave nodes.

To install the Closed Captioning Service:

1. If you have not already done so, navigate to the directory containing the installation script:

   ```
   cd /<path>
   ```

2. Run the CC Service installation script:

   ```
   ./install.sh
   ```

   The period-slash “./” in this command tells Linux to look for the script in the current directory.

   The end of the CCS installation process should indicate a successful installation:

   ```
   Installed:
     avid-ccc.x86_64 0:1.1.271-1
     avid-ccc-anc.x86_64 0:1.0.66-1
     avid-ccc-cluster-config.x86_64 0:1.0.1-1
     avid-interplay-central-closed-captioning.noarch 0:2.9.5-1
     avid-interplay-central-interplay-cc.noarch 0:2.9.7-1


   Complete!
   ```

3. Verify the success of the installation using the Linux rpm command:

   ```
   rpm -qa | grep avid-ccc
   ```

   The output should include the following lines:

   ```
   avid-ccc-anc-<version>.x86_64
   avid-ccc-cluster-config-<version>.x86_64
   avid-ccc-<version>.x86_64
   ```

4. As detailed in the MCS v2.9.1 ReadMe, the Closed Captioning service v2.9.0 does not automatically create the AvidCCC cluster resource as it should. Complete the following steps to create the resource manually:

   a. Stop the avid-ccc service:

      ```
      service avid-ccc stop
      ```

      Repeat this step on the cluster master and slave nodes.

   b. Since the service will be controlled through Pacemaker as a resource, you must configure the service to be off at system boot:

      ```
      chkconfig avid-ccc off
      ```

      Repeat this step on the cluster master and slave nodes.

   c. On the master node only, create the AvidCCC cluster resource by launching the following script:

      ```
      /opt/avid/cluster/bin/ccc-cluster setup
      ```

Bringing the Cluster Online

With the Closed Captioning Service installed on the Master and Slave nodes, bring the cluster back online. Make sure to follow the order represented below.

To bring the cluster online:

1. First, bring the master node back online:

   ```
   crm node online <node name>
   ```

2. Next, bring the slave node online:

   ```
   crm node online <node name>
   ```

3. Finally, bring any load-balancing nodes online:

   ```
   crm node online <node name>
   ```

Checking on the Cluster Status

With the Closed Captioning Service installed and the cluster resources back online, verify that the new AvidCCC resource has appeared and that the cluster is free of errors.

To verify the cluster status:

1. Use the Cluster Resource Monitor to verify the status of the cluster:

   ```
   crm_mon -f
   ```

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Verify that the new AvidCCC resource is started on the master node.
   - Review the fail-counts for the cluster resources.

2. If there are fail-counts listed, run the Cluster Resource Manager cleanup command to reset them:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   <*rsc*> is the resource name of interest: AvidCCC, AvidIPC, pgsqlDB (or another)

   <*node*> (optional) is the node of interest

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the "everywhere" form of the resource.

For example, to reset the fail-count for AvidAll resource, issue the following command:

```
crm resource cleanup AvidAllEverywhere
```

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

Uninstalling the Closed Captioning Service

In the event that you need to disable the Closed Captioning functionality, use the following process to uninstall the CC Service. This process will disconnect any users currently working on the system. Make sure all users save their work prior to completing this process.

To uninstall the CC Service on a single server:

1. Navigate to the directory containing the CC Service installation files:

   ```
   cd /<path>
   ```

2. Run the CC Service uninstall script:

   ```
   ./uninstall.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   The CC Service is uninstalled and the avid-interplay-central service is restarted.

To uninstall the CC Service on a cluster:

1. Verify the current Master, Slave and load balancing nodes.

   For details, see "Identifying the Master, Slave and Load-Balancing Nodes" on page 168.

2. Take the cluster offline.

   For details, see "Taking the Cluster Offline" on page 169.

3. Starting with the master node, navigate to the directory containing the CC Service installation files:

   ```
   cd /<path>
   ```

4. Run the CC Service uninstall script:

   ```
   ./uninstall.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

5. Repeat steps 3 and 4 on the slave node.

MediaCentral Platform Services v2.3 through v2.6 required the Closed Captioning Service to be installed on all cluster nodes. If you are uninstalling an older version of the software, repeat steps 3 and 4 to uninstall the service on all load-balancing nodes.

6. Bring the cluster back online.

   For details, see "Bringing the Cluster Online" on page 170.

7. Use the Cluster Resource Monitor to verify the status of the cluster:

   ```
   crm_mon -f
   ```

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Verify that the AvidCCC resource has been removed.
   - Verify that the AvidIPC resource is online on the master node.
   - Review the fail-counts for the cluster resources.

8. If there are fail-counts listed, run the Cluster Resource Manager cleanup command to reset them:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   <rsc> is the resource name of interest: AvidIPC, pgsqlDB (or another)

   <node> (optional) is the node of interest

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the "everywhere" form of the resource.

For example, to reset the fail-count for AvidAll resource, issue the following command:

```
crm resource cleanup AvidAllEverywhere
```

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

9 Customizable Logger

Chapter Overview

The purpose of this chapter is to guide you through the installation and configuration of the MediaCentral Customizable Logger introduced with MediaCentral Platform Services v2.7.

The following table describes the topics that are covered in this chapter:

Step	Task	Time Est.
1	Preparing the Software Package	5 min
	Process for copying and unzipping the installer.	
2	Installing the Customizable Logger on a Single Server	5 min
	Process for installing the Customizable Logger on a single MCS server.	
3	Installing the Customizable Logger in a Cluster	15 min
	Process for installing the Customizable Logger in an MCS cluster.	
4	Configuring the Customizable Logger	5 min
	Once the software is installed, the Logger settings must be updated.	
5	Verifying the Installation	5 min
	Covers the areas where administrators can verify the installation.	
- -	Upgrading the Customizable Logger	2 min
	This section includes notes related to upgrading an existing installation.	
- -	Uninstalling the Customizable Logger	15 min
	Process for removing the Customizable Logger software from the MediaCentral server.	
- -	Working with the Customizable Logger	*varies*
	Topics and concepts that are not covered in the installation process.	

The Customizable Logger adds new functionality to MediaCentral UX in the form of the Logging Controls pane which enables users to create project-specific layouts that can greatly enhance and streamline logging workflows. This feature is similar to Media | Distribute in that the software is not included with a standard MCS installation. The plug-in must be purchased and installed separately.

The traditional Logging pane creates marker metadata that is stored with the original assets in the Interplay Production or Interplay MAM database. In contrast, the data created through the Customizable Logger is stored locally on the MCS servers in a non-sharded MongoDB database.

The Customizable Logger installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and sign off during the installation or upgrade procedures.

For more information on this feature, see “Customizable Logger” section of the *Avid MediaCentral | UX User’s Guide*.

Preparing the Software Package

Before you can start the installation, you must obtain the Customizable Logger software and copy it to your MediaCentral server(s). If you have a cluster configuration, complete steps below on the master and slave nodes only.

To prepare the software package:

1. Ensure that you have obtained and copied the software to the MCS server(s). If you have not completed these tasks, see “Obtaining the Software” on page 21 and “Copying Software to the MCS Server” on page 238 for instructions.
2. Navigate to the directory where the installer has been copied. Example:

   ```
   cd /media/installers
   ```

3. If necessary, unzip the installer:

   ```
   unzip MediaCentral_Customizable_Logger_<x.x.x>_Linux.zip
   ```

4. Navigate to the newly created directory:

   ```
   cd MediaCentral_Customizable_Logger_<x.x.x>_<build>_Linux
   ```

Installing the Customizable Logger on a Single Server

This section details the steps required to install the Customizable Logger on a single-server.

To install the Customizable Logger:

1. If you have not already done so, navigate to the directory containing the installation script:

   ```
   cd /<path>
   ```

2. Run the Customizable Logger installation script:

   ```
   ./install.sh
   ```

   The period-slash “./” in this command tells Linux to look for the script in the current directory.

   The process should complete with messages similar to the following, indicating a successful installation:

   ```
   Complete!
   Stopping avid-interplay-central  Avid Interplay Central process is running
   Avid Interplay Central webinterface is available                     [ OK ]

   Starting avid-interplay-central  Avid Interplay Central is not running
   Avid Interplay Central process has been started.
   Wait for Interplay Central web interface...
   Avid Interplay Central has been started successfully (15 seconds)    [ OK ]
   ```

3. Once the software is installed, proceed to “Configuring the Customizable Logger” on page 177 to update the System Name associated with the logging index.

Installing the Customizable Logger in a Cluster

In a cluster deployment, the Customizable Logger is installed on the master and slave nodes only.

The cluster installation process involves the following steps:

- Preparing the Software Package
- Verifying Prerequisites
- Installing the Customizable Logger
- Checking on the Cluster Status

Verifying Prerequisites

Prior to installing the Customizable Logger, verify the following:

- MCS is installed and configured on all servers in the cluster.
- All cluster resources should be online and free of errors.

  Use “crm_mon -f” to verify the cluster status.

Unlike installations such as the Closed Captioning Service or the MAM Connector, all cluster nodes must be online prior to installing the Customizable Logger. The Customizable Logger integrates with the MongoDB database located on the master and slave nodes and all related services must be active during the installation process.

Installing the Customizable Logger

Complete the following process on the cluster master and slave nodes. Install the software on the slave node first, followed by the master node.

To install the Customizable Logger:

1. If you have not already done so, navigate to the directory containing the installation script:

   ```
   cd /<path>
   ```

2. Run the Customizable Logger installation script:

   ```
   ./install.sh
   ```

   The period-slash “./” in this command tells Linux to look for the script in the current directory.

   The process should complete with a message similar to the following, indicating a successful installation:

   ```
   Complete!
   ```

3. Repeat steps 1 and 2 on the master node.

   The process should complete with a similar “Complete!” message, but will also include information related to updates for the MongoDB database and a restart of the AvidIPC resource similar to the following:

```
Complete!

updates path detected at /opt/avid/share/avid/db/migrations/

********** UPDATE avid-customizable-logging:0 --- Initial setup of mongo
db/collections for service avid-customizable-logging **********

Launch step_00: Drop db: customizable-logging
                Execution time: a few seconds
Launch step_01: Creates indexes for collection: assignment
                Execution time: a few seconds
Launch step_11: Creates indexes for collection: event
                Execution time: a few seconds
Launch step_21: Creates indexes for collection: folder
                Execution time: a few seconds
Launch step_31: Creates indexes for collection: preset
                Execution time: a few seconds
Launch step_41: Creates indexes for collection: segment
                Execution time: a few seconds
Launch step_51: Imports data into new collection: system
                Execution time: a few seconds
Launch step_61: Imports data into new collection: version
                Execution time: a few seconds

********** UPDATE avid-customizable-logging:0 --- Successful. Update
execution time: a few seconds

Done. System is up-to-date. Total execution time: a few seconds

Set 'AvidIPC' option: id=AvidIPC-meta_attributes-target-role set=AvidIPC-
meta_attributes name=target-role=stopped

Waiting for 1 resources to stop:

 * AvidIPC

Deleted 'AvidIPC' option: id=AvidIPC-meta_attributes-target-role
name=target-role

Waiting for 1 resources to start again:

 * AvidIPC
```

Checking on the Cluster Status

With the Customizable Logger installed, verify that all cluster resources are running and that the Cluster Resource Monitor is free of errors.

To verify the cluster status:

1. Use the Cluster Resource Monitor to verify the status of the cluster:

   `crm_mon -f`

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Review the fail-counts for the cluster resources.

2. If there are fail-counts listed, run the Cluster Resource Manager cleanup command to reset them:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   <*rsc*> is the resource name of interest: AvidIPC, pgsqlDB (or another)

   <*node*> (optional) is the node of interest

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the "everywhere" form of the resource.

   For example, to reset the fail-count for AvidAll resource, issue the following command:

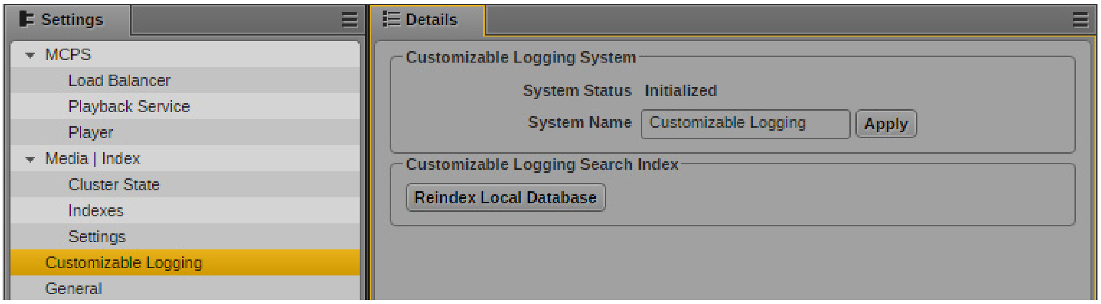
   ```
   crm resource cleanup AvidAllEverywhere
   ```

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

3. Once the software is installed, proceed to "Configuring the Customizable Logger" on page 177 to update the System Name associated with the logging index.

Configuring the Customizable Logger

The installation of the Customizable Logger adds a new line item to the MediaCentral UX System Settings called "Customizable Logging".



Customizable Logging System

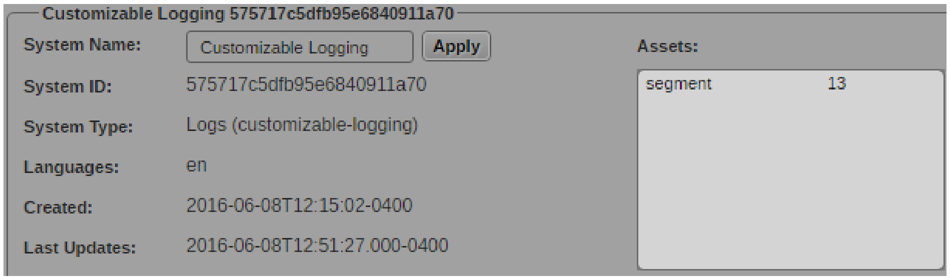
System Status: Initialized

System Name: Customizable Logging

Customizable Logging Search Index

When Customizable Logger is installed, "Customizable Logging" is set as the default System Name for the logging index. For systems configured with Media Index, the System Name appears in two locations:

- System Name field for the index in System Settings > Media Index > Indexes:



Customizable Logging 575717c5dfb95e6840911a70

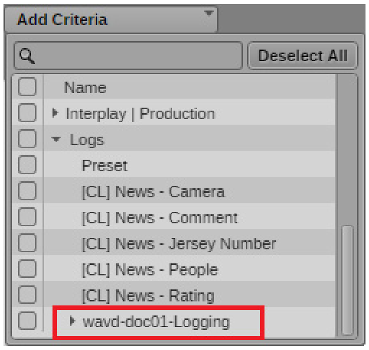
System Name:	Customizable Logging
System ID:	575717c5dfb95e6840911a70
System Type:	Logs (customizable-logging)
Languages:	en
Created:	2016-06-08T12:15:02-0400
Last Updates:	2016-06-08T12:51:27.000-0400

Assets:

segment	13

The System ID is also shown in this view. This field is cannot be edited.

- Searchable field for Indexed searches:



For systems configured with Media Index, the System Name appears in a location that is exposed to users. Therefore it is important to change the name to a more user-friendly value. This becomes even more important for sites that participate in multi-zone configurations where remote users need to be able to easily associate the System Name with a zone's location.

Even if your system is not configured with Media Index at this time, it is still good practice to assign a customized System Name. This enables a smoother transition for any future Media Index workflow by eliminating the need to re-index the Customizable Logger database.

The System Name will appear in the two above locations only after the Customizable Logger is used to create searchable data for the first time.

To customize the System Settings:

1. Using Chrome or another qualified browser, sign into MediaCentral UX as a user with administrator-level access.
2. Select System Settings from the Layout menu.
3. In the Settings pane, select Logging Controls.
4. Enter a customized System Name in the text box and click Apply.

   Examples: <*hostname*>-Logger or NewYork-Logger

Verifying the Installation

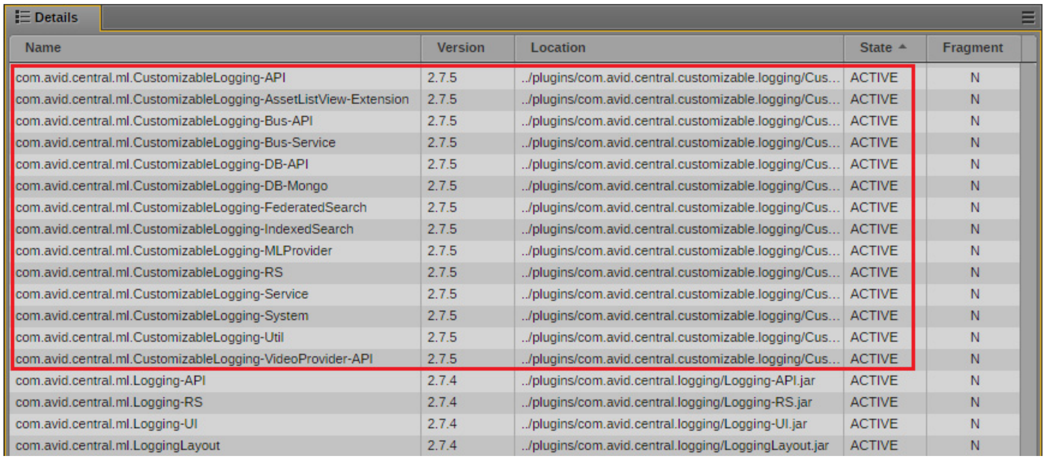
Once the installation is complete, users should verify the installation and test basic functionality. Systems configured with Media Index can further verify that an index has been created for the logging data contained in the MongoDB database.

The logging index will appear after the Customizable Logger is used to create searchable data for the first time. In other words, create some custom logging data and then verify the index data.

To verify the installation:

1. Using Chrome or another qualified browser, sign into MediaCentral UX as a user with administrator-level access.
2. Select System Settings from the Layout pull-down menu.
3. In the Settings pane, select Modules.
4. Click the Name column in the right pane to sort the information by Name.

5. Use the scroll bar to navigate to the “com.avid.central.CustomizableLogging” section of the list. There should be multiple CustomizableLogging modules listed.



Name	Version	Location	State ▲	Fragment
com.avid.central.ml.CustomizableLogging-API	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-AssetListView-Extension	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-Bus-API	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-Bus-Service	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-DB-API	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-DB-Mongo	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-FederatedSearch	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-IndexedSearch	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-MLProvider	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-RS	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-Service	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-System	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-Util	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-VideoProvider-API	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.Logging-API	2.7.4	../plugins/com.avid.central.logging/Logging-API.jar	ACTIVE	N
com.avid.central.ml.Logging-RS	2.7.4	../plugins/com.avid.central.logging/Logging-RS.jar	ACTIVE	N
com.avid.central.ml.Logging-UI	2.7.4	../plugins/com.avid.central.logging/Logging-UI.jar	ACTIVE	N
com.avid.central.ml.LoggingLayout	2.7.4	../plugins/com.avid.central.logging/LoggingLayout.jar	ACTIVE	N

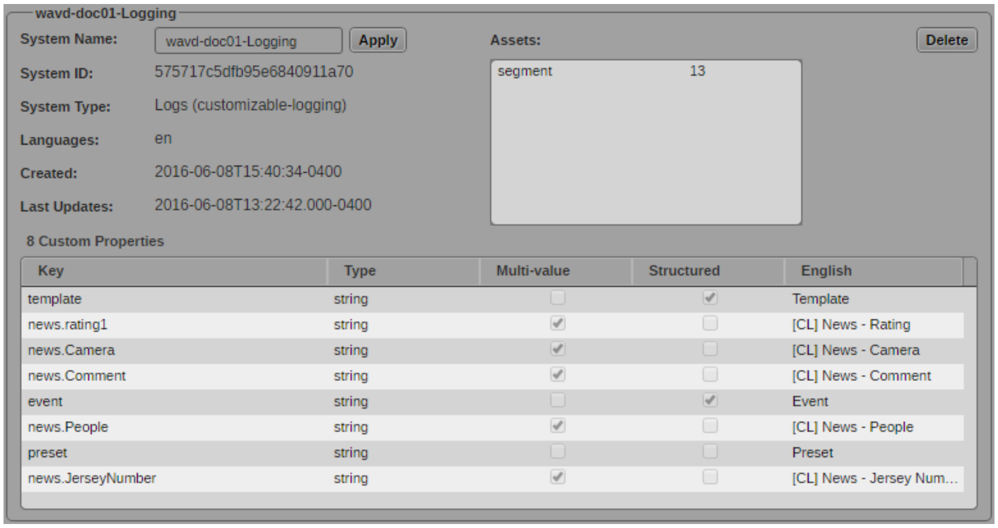
All modules must show a status of ACTIVE in the State column.

Version numbers will vary from this example, depending on the version of the installed software.

6. Select either the Log, Cut, Rundown or Story options from the Layout pull-down menu.
7. Verify that the Logging Controls pane is listed in the Panes menu.

To verify integration with Media Index:

1. Using Chrome or another qualified browser, sign into MediaCentral UX as a user with administrator-level access.
2. Select System Settings from the Layout menu.
3. In the Settings pane, select Media | Index > Indexes.
4. Verify that Details pane shows a new index for the Customizable Logger.



wavd-doc01-Logging

System Name: wavd-doc01-Logging

System ID: 575717c5dfb95e6840911a70

System Type: Logs (customizable-logging)

Languages: en

Created: 2016-06-08T15:40:34-0400

Last Updates: 2016-06-08T13:22:42.000-0400

Assets:

segment	13

8 Custom Properties

Key	Type	Multi-value	Structured	English
template	string	□	☑	Template
news.rating1	string	☑	□	[CL] News - Rating
news.Camera	string	☑	□	[CL] News - Camera
news.Comment	string	☑	□	[CL] News - Comment
event	string	□	☑	Event
news.People	string	☑	□	[CL] News - People
preset	string	□	□	Preset
news.JerseyNumber	string	☑	□	[CL] News - Jersey Num...

If you do not see an index for the Customizable Logger, you might need to use the scroll bar on the right of the Details pane to reveal additional indexes.

Upgrading the Customizable Logger

The process for upgrading an existing installation and performing a new installation of the Customizable Logger are the same. The upgrade process simply overwrites the appropriate files.

When upgrading an existing installation, note the following:

- The Customizable Logger installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and sign off during the installation or upgrade procedures.
- During the upgrade process, you might see the following message:

  ```
  Updates path detected at /opt/avid/share/avid/db/migrations/
  Available updates list is empty. Nothing to execute.
  ```

  If the updated version of the software does not include a MongoDB schema change, this message is normal and can be ignored.

Uninstalling the Customizable Logger

In the event that you need to disable the functionality added by the Customizable Logger, use one or more of the following processes to uninstall the software. For systems configured with Media Index, users can optionally remove the Customizable Logger index to prevent search results from returning any custom logging data. Finally, if desired, the MongoDB database can be reset to a new, clean state.

This process will disconnect any users currently working on the system. Make sure all users save their work prior to completing this process.

Uninstalling the Customizable Logger on a Single Server

To uninstall the software on a single server:

1. Navigate to the directory containing the Customizable Logger installation files:

   ```
   cd /<path>
   ```

2. Run the Customizable Logger uninstall script:

   ```
   ./uninstall.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   The software is uninstalled and the avid-interplay-central service is restarted.

3. If desired, proceed to "Removing the Logging Index" on page 181 to reset the index data.

Uninstalling the Customizable Logger on a Cluster

To uninstall the Customizable Logger on a cluster:

1. Verify the current Master, Slave and load balancing nodes. For more information, see "Identifying the Master, Slave and Load-Balancing Nodes" on page 268.

2. Starting with the master node, navigate to the directory containing the Customizable Logger installation files:

   ```
   cd /<path>
   ```

3. Run the Customizable Logger uninstall script:

   ```
   ./uninstall.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

4. Repeat steps 2 and 3 on the slave node.

5. Use the Cluster Resource Monitor to verify the status of the cluster:

   ```
   crm_mon -f
   ```

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Verify that the AvidIPC resource is online on the master node.
   - Review the fail-counts for the cluster resources.

6. If there are fail-counts listed, run the Cluster Resource Manager cleanup command to reset them:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   <*rsc*> is the resource name of interest: AvidIPC, pgsqlDB (or another)

   <*node*> (optional) is the node of interest

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the "everywhere" form of the resource.

For example, to reset the fail-count for AvidAll resource, issue the following command:

```
crm resource cleanup AvidAllEverywhere
```

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

7. If desired, proceed to "Removing the Logging Index" on page 181 to reset the index data.

Removing the Logging Index

This process will remove the Customizable Logger index only; the actual data contained in the MongoDB database is unaffected. System administrators must complete a reindex of the database to recover this information. Reindexing the database can be a time consuming process for systems with large amounts of logging data.

To remove the logging index:

1. Using Chrome or another qualified browser, sign into MediaCentral UX as a user with administrator-level access.
2. Select System Settings from the Layout menu.
3. In the Settings pane, select Media | Index > Indexes.
4. Find the Customizable Logger index in the Details pane and click the Delete button to remove the index.
5. If desired, proceed to "Resetting the MongoDB Database" on page 182 to remove all logging data from the system.

Resetting the MongoDB Database

⚠ **This process will delete all logging information from the MongoDB database. Unless you have a backup, the information is lost and cannot be recovered.**

Run the following command to drop the logging information from the database and create a new, clean database. If you are in a cluster configuration, this command must be completed on the cluster master node.

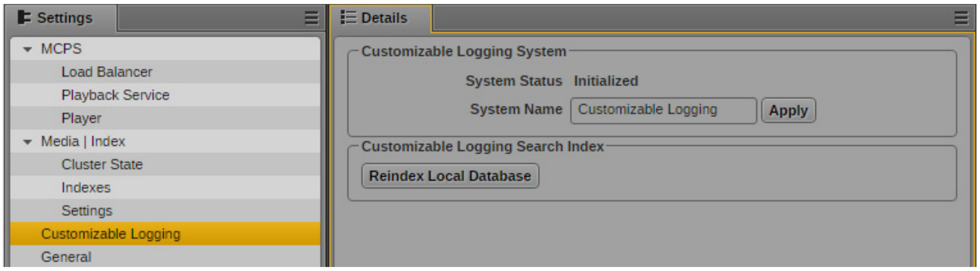
```
/opt/avid/bin/avid_cl_db_recreate
```

Working with the Customizable Logger

This section provides additional details on the Customizable Logger (CL).

Understanding the System Settings

When installed, the service adds a “Customizable Logging” line item to the list of System Settings.



System Status Initialized

System Name Customizable Logging

- **System Name**: As previously described, this field is used to assign a custom name to the index. The System Name appears in the list of searchable fields in an Indexed search.
- **Reindex Local Database**: Clicking this button will perform the following actions:
  - Current index of all Customizable Logger data is deleted. The deletion applies to the *index* of the data only. The actual data stored in the MongoDB database is unaffected.
  - A new index is created for use with Media Index, Indexed searches.
  - All custom logging data is imported to the new index from MongoDB.

  The re-index process can take a significant amount of time for sites that have a large amount of logging data. Once the process is complete a “Success – Reindex completed” message is displayed.

Backing Up and Restoring the Customizable Logger Database

If desired, users can manually back up and restore the logging information stored in the MongoDB database. The information below details how to complete those processes. Additionally, information is provided on how to delete all logger information from the database; reverting it to a “new” state.

To back up the logger database:

Run the following command to create a backup of the Customizable Logger database:

```
/opt/avid/bin/avid_cl_db_dump
```

Backups of the database are created in the /var/lib/avid/db/dumps directory and are named similar to the following:

```
customizable-logging-20160608_125833Z.mongo.tar.gz
```

To restore the logger database:

1. The restore command assumes that the backup file is located at /var/lib/avid/db/dumps. If it is not, you must first copy the backup to this directory:

   ```
   cp /<path>/<filename> /var/lib/avid/db/dumps
   ```

   For example:

   ```
   cp /tmp/customizable-logging-20160913_205332Z.mongo.tar.gz /var/lib/avid/
   db/dumps
   ```

2. Run the following command to restore a backup copy of the Customizable Logger database:

   ```
   /opt/avid/bin/avid_cl_db_restore <filename_without_extension>
   ```

   For example:

   ```
   /opt/avid/bin/avid_cl_db_restore customizable-logging-
   20160608_125833Z.mongo
   ```

   Make sure that you do not include the .tar.gz extension in this command.

   The restore process prints a series of messages to the screen and completes with a “done” statement:

   ```
   2016-10-04T11:34:36.052-0400    finished restoring customizable-
   logging.system (1 document)
   2016-10-04T11:34:36.052-0400    finished restoring customizable-
   logging.event (2 documents)
   2016-10-04T11:34:36.052-0400    done
   ```

To remove all logging information from the database:

Run the following command to drop the logging information from the database and create a new, clean database:

```
/opt/avid/bin/avid_cl_db_recreate
```

⚠ **This command will delete all logging information from the MongoDB database. Unless you have a backup, the information is lost and is not recoverable.**

Troubleshooting

For troubleshooting information, see the Troubleshooting MediaCentral | UX Customizable Logger article on the Avid Knowledge Base.

10 Maestro UX Plug-In

Chapter Overview

For workflows that include Maestro, a Maestro UX plug-in is available for Avid MediaCentral Platform Services v2.7.1 and later. This chapter guides you through the installation of the plug-in software on both the MediaCentral Platform Services server and the Maestro server.

The following table describes the topics covered in this chapter:

Step	Task	Time Est.
1	Before You Begin	5 min
	Verify that you have all perquisite information prior to starting the software installation.	
2	Installing Software on the Maestro Server	20 min
	This section provides instructions for installing the Maestro Render Server application and associated services.	
3	Verifying the Installation Through the ACS Monitor	10 min
	Once the Maestro services are installed, the ACS Monitor is used to verify the installation.	
4	Configuring the Maestro Render Server	10 min
	A Maestro application for configuring system operation.	
5	Installing the Plug-Ins on the MCS Server	15 min
	Process for installing the software on the MediaCentral Platform Services server.	
6	Configuring the MediaCentral UX System Settings	5 min
	After the software is installed, settings must be updated to enable communication between the MCS and Maestro server.	
- -	Upgrading Maestro UX	30 min
	Process for upgrading the Maestro UX software on both the MediaCentral server and the Maestro server.	
- -	Uninstalling Maestro UX	10 min
	Process for removing the Maestro UX software from both the MediaCentral server and the Maestro server.	
- -	Additional Information	*varies*
	Additional topics regarding Maestro UX.	

Maestro is a universal controller that lets you create and manage template-based, on-air 3D graphics. The Maestro UX plug-in for MediaCentral Platform Services provides a connection to the Maestro Asset database through the MediaCentral UX Launch pane. Through this pane, drag and drop workflows between Maestro and Avid iNEWS or Interplay MAM are now possible.

Currently, the Maestro UX plug-in is supported with iNEWS and Interplay MAM workflows only.

For additional details regarding features and usage of the Maestro UX plug-in, see the *Avid MediaCentral | UX User's Guide* and the *Avid Maestro Users Guide* v7.2 or later.

Before You Begin

The Maestro UX plug-in installation process requires new software to be added to both the Maestro server and the MediaCentral Platform Services server(s). Before installing the Maestro UX plug-in software, verify that you have identified the following:

- The IP address of the MediaCentral Platform Services server. If running a cluster configuration, identify the IP address assigned to the cluster (virtual IP).
- The IP address, host name, or FQDN of the server running the Maestro Asset database.
- The user and password used to access the Maestro Asset database.
- The IP address, host name, or FQDN of the Maestro Render Server database.
- The user and password used to access the Maestro Render Server database.
- The ID of the Orad MOS Gateway. This value can be found in the MOSGatewayGUI tool on the Maestro server.

Installing Software on the Maestro Server

The Maestro server is a dedicated Windows-based PC that runs Graphics Suite components required for Maestro workflows. Some of these components include: MS SQL for Maestro DB, Shared Data, MOS Gateway, License Server, Render Server, and others.

To enable communication between MediaCentral Platform Services and Maestro, multiple pieces of software must be installed on the Maestro server. These services include:

- Maestro Render Server
- Render Server Service
- Maestro Bus Services (includes the following components):
  - Asset Access Service - Enables the Maestro UX plug-in to access the Maestro Database. This enables users access to the database to browse for graphic assets.
  - Data Link Service - Provides access to data sources in the SQL database on the Maestro server. These sources are used to populate graphics.
  - Media Browser Service - Provides access to Maestro assets (clips and images).
  - Maestro Monitor - A tool for controlling the above services.

This section guides you through the installation and configuration of the Maestro server for integration with MediaCentral Platform Services.

Preparing the Software Package

Before you can start the installation, you must obtain the software and copy it to the Maestro server.

To prepare the software package:

1. The Graphics Suite installation package includes the software required to enable workflows between Maestro and MediaCentral Platform Services. Copy the installer to the desktop of the Maestro server.
2. Unzip the GraphicsSuite_<*version*>.zip file to its own folder.
3. In addition to the Avid provided packages, the server running the Data Link Service must also be running Microsoft Visual C++ Runtime v14.0 (x64). If your server does not already have this software installed, download and install it on your Maestro server from the Microsoft website:

   https://www.microsoft.com/en-us/download/details.aspx?id=48145

Installing the Maestro Render Server

This package installs the Server and Client software for the Maestro Render Server and the Maestro Render Manager. These applications allow users to manage render templates and start the Render Server Engine.

To install the Maestro Render Server:

1. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Render Server installer "Maestro64_<*version_build*>.exe".
2. The "Welcome to Maestro Render Server (x64) Setup" screen appears.

   Click Next.
3. In the "Setup Type" window, select the Typical button and click Next.

   If required, the Custom Setup option allows you to select a custom installation path. For consistency, selecting the Typical installation option is recommended.
4. In the "MaestroRenderServer components categories" window, select the following options as required by your installation:
   - Server components: This option installs the Maestro Render Server components on the local hard drive.
   - Client component (optional): This option installs the Maestro Render Server COM API component used by the Render Server Service.

   The Maestro Render Server **Client** components must be installed on the server that you plan to install the Render Server Service. The Maestro Render Server **Server** components must also be installed prior to installing the Render Server service. However, the Client software does not necessarily need to be installed on the same system as the Server software.
5. Click Next.
6. In the "MaestroRenderServer - Database access" window, enter the following information:
   - **Host**: Enter the host name of the server running the MSSQL Maestro Render Server database as well as the instance name of the database.

     Example: wavd-maestro01\maestro

The Maestro Render Server database is different than the Maestro Asset database. Verify that you are entering the correct information on this page.

- **User**: Enter the SQL user name to be used by the Render Server Service to access the database.

  Example: sa

- **Password**: Enter the password for the above user.
- **Database name**: Enter the name of the Maestro Render Server database.

  Example: MaestroRenderServer (default)

7. Click Next.
8. If the installer detects that the MaestroRenderServer database already exists, a window appears asking if you want to either use the existing database or create a new database.

   Select the button to either “Use existing” or “Create new”.

⚠ **If you select “Create new” and an existing database is in place, the database will be replaced and the original data is unrecoverable. Make sure to select the correct option in this window.**

9. Click Next.
10. In the “Maestro Database Server” window, select the Native 2 option. This is the only database format supported by Maestro.

    Do not select the “use trusted connection” option (typical for most installations).

11. In the “Access to Maestro Database” window, enter the following information:
    - **Server**: Enter the IP address or host name of the server running the MSSQL Maestro Asset database as well as the instance name of the database.

      Example: wavd-maestro01\maestro

    - **User**: Enter the SQL user name to be used by the Maestro Bus Service to access the database.

      Example: sa

    - **Password**: Enter the password for the above user.
12. Click Next.
13. In the “Ready to Install” window, review the information you have entered and click Next to begin the installation.

    If the installation summary contains any errors, click the Back button to return to a previous step and correct the error.

14. Once the installation is complete, click the Finish button to exit the installer.

Installing the Render Server Service

When selecting the Render button in the MediaCentral UX “Maestro Browser” pane, the Render Server Service is used to generate graphic image sequences for preview.

As a reminder, the Maestro Render Server Client components must be installed on the server that runs the Render Server Service. The Client components must be installed before installing the service.

To install the Render Server Service:

1. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Render Server Service installer “RenderServerService_<*version_build*>.exe”.
2. The “Welcome to RenderServerService Setup” screen appears.

   Click Next.
3. In the “Setup Type” window, select the Typical button and click Next.

   If required, the Custom Setup option allows you to select a custom installation path. For consistency, selecting the Typical installation option is recommended.
4. In the “RenderServerService ACS Gateway settings” window, enter the following information:
   - **Host**: Enter the IP address of the MediaCentral Platform Services server. If this is a cluster configuration, enter the IP address associated with the cluster (virtual IP address).
   - **Port**: Enter the port number used to communicate with the ACS Gateway. Port 9900 is typically used for this communication.

   Click Next to continue.
5. In the “Access to RenderServerService Database” window, enter the following information:
   - **Server**: Enter the IP address or host name of the server running the MSSQL MaestroRenderServer database as well as the instance name of the database.

     Example: wavd-maestro01\maestro

The MaestroRenderServer database is different than the Maestro Asset database. Verify that you are entering the correct information on this page.

   - **User**: Enter the SQL user name to be used by the Render Server Service to access the database.

     Example: sa
   - **Password**: Enter the password for the above user.
   - **Name**: Enter the name of the MaestroRenderServer database.

     Example: MaestroRenderServer (default)
   - If you wish to verify the above settings, select the “verify database server connection” check box.

   Click Next.

   If you selected the check box to check the connection, the test is completed at this time. If the test fails to connect to the server, a dialog box is displayed indicating a problem with the configuration. If necessary, press the Back button to review and correct the information.
6. In the “Ready to Install” window, review the information you have entered and click Next to begin the installation.

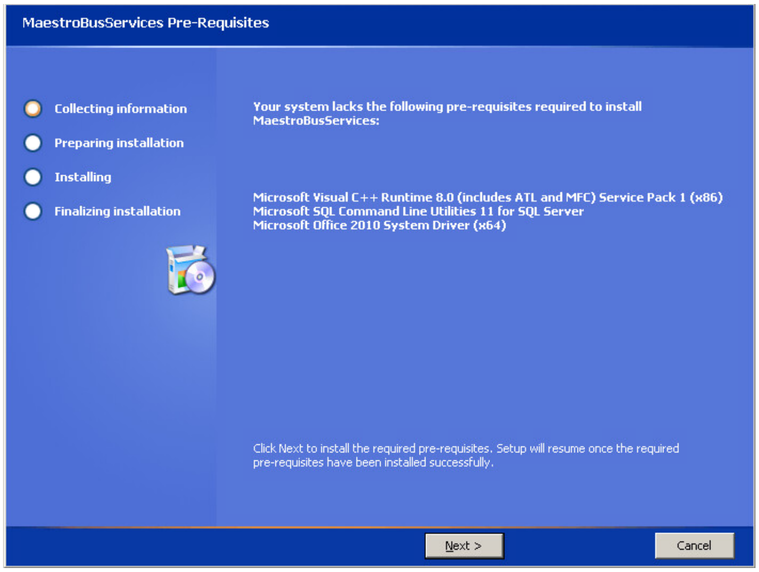
   If the installation summary contains any errors, click the Back button to return to a previous step and correct the error.
7. Once the installation is complete, click the Finish button to exit the installer.

Installing the Maestro Bus Services

This package installs the Asset Access Service, Data Link Service, Media Browser Service, and the Maestro Monitor on the Maestro server.

To install the Maestro Bus Service:

1. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Bus Services installer "MaestroBusServices_<*version_build*>.exe".
2. Prior to installing the Maestro services, the installer checks for all required software packages. Any prerequisites that have not been installed are listed on the "MaestroBusServices Pre-Requisites" screen (as shown in the following example):

   MaestroBusServices Pre-Requisites

   Your system lacks the following pre-requisites required to install MaestroBusServices:

   Microsoft Visual C++ Runtime 8.0 (includes ATL and MFC) Service Pack 1 (x86)
   Microsoft SQL Command Line Utilities 11 for SQL Server
   Microsoft Office 2010 System Driver (x64)

   Click Next to install the required pre-requisites. Setup will resume once the required pre-requisites have been installed successfully.

   If prompted, click Next to install the missing software packages.

   In most cases these packages are already installed on your Maestro server and you should not be prompted to install additional software.
3. The "Welcome to MaestroBusServices Setup" screen appears.

   Click Next.
4. In the "License Agreement" window, select the check box to accept the license agreement and click Next to continue.
5. In the "Setup Type" window, select the Typical button and click Next.

   If required, the Custom Setup option allows you to select a custom installation path. For consistency, selecting the Typical installation option is recommended.
6. In the "MaestroBusServices ACS Gateway settings" window, enter the following information:

   - **Host**: Enter the IP address of the MediaCentral Platform Services server. If this is a cluster configuration, enter the IP address associated with the cluster (virtual IP address).
   - **Port**: Enter the port number used to communicate with the ACS Gateway. Port 9900 is typically used for this communication.

   Click Next to continue.
7. In the "Access to MaestroBusServices Database" window, enter the following information:

   - **Server**: Enter the IP address or host name of the server running the MSSQL Maestro Asset database as well as the instance name of the database.

     Example: wavd-maestro01\maestro

- **User**: Enter the SQL user name to be used by the Maestro Bus Service to access the database.

  Example: sa
- **Password**: Enter the password for the above user.
- **Name**: Enter the name of the Maestro Asset database.

  Example: maestro_3 (default)
- If you wish to verify the above settings, select the “verify database server connection” check box.

Click Next.

If you selected the check box to check the connection, the test is completed at this time. If the test fails to connect to the server, a dialog box is displayed indicating a problem with the configuration. If necessary, press the Back button to review and correct the information.

8. In the “Ready to Install” window, review the information you have entered and click Next to begin the installation.

   If the installation summary contains any errors, click the Back button to return to a previous step and correct the error.
9. Once the installation is complete, click the Finish button to exit the installer.

Enabling the Services

With the software installed, use the Maestro Monitor application to start the required services.

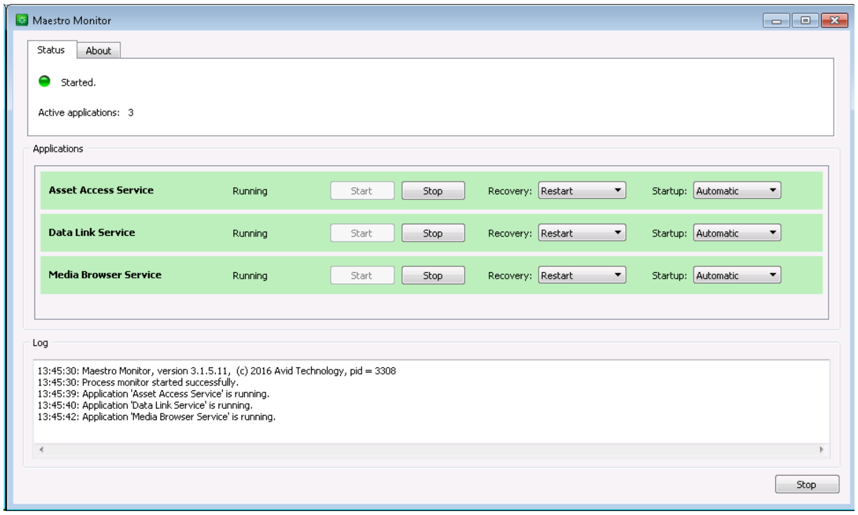
To enable the Maestro services:

1. Open the Maestro Monitor application:
   - From the Windows Start menu at:

     Start > All Programs > Orad > MaestroMonitor
   - Through the executable in the system file structure:

     C:\Orad\MaestroBusServices\MaestroMonitor.exe

   The Monitor tool opens, showing the services and their current status:



Started.

Active applications: 3

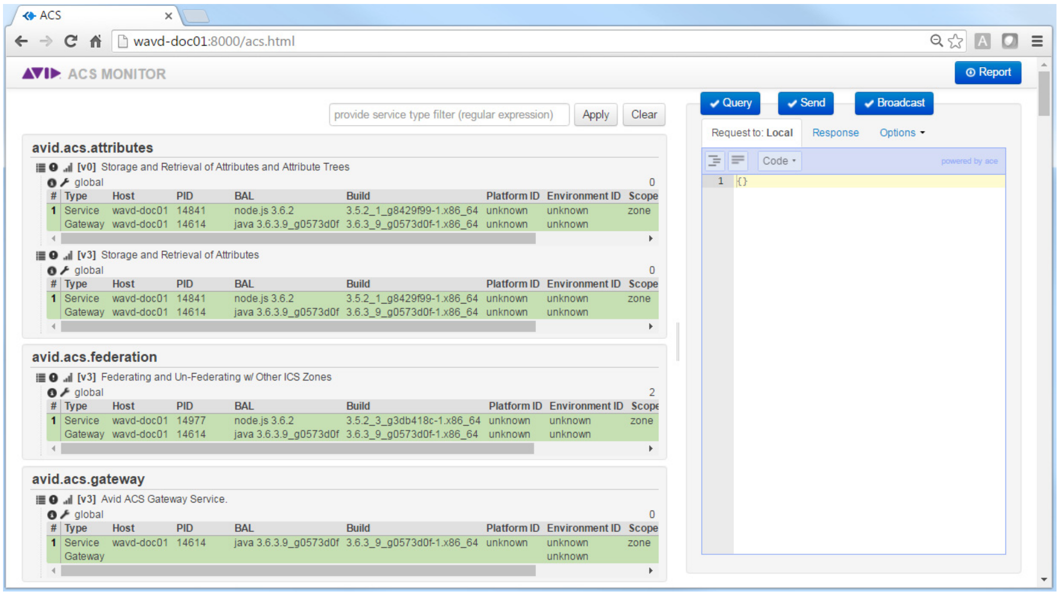
Asset Access Service	Running	Start	Stop	Recovery: Restart	Startup: Automatic
Data Link Service	Running	Start	Stop	Recovery: Restart	Startup: Automatic
Media Browser Service	Running	Start	Stop	Recovery: Restart	Startup: Automatic

```
13:45:30: Maestro Monitor, version 3.1.5.11,  (c) 2016 Avid Technology, pid = 3308
13:45:30: Process monitor started successfully.
13:45:39: Application 'Asset Access Service' is running.
13:45:40: Application 'Data Link Service' is running.
13:45:42: Application 'Media Browser Service' is running.
```

2. Verify that the Recovery mode for each service is set to “Restart” and that the Startup mode is set to “Automatic”.
3. If any services are not running, click the Start button in the lower-right corner of the window to start all services.

Verifying the Installation Through the ACS Monitor

Avid provides a user interface called the Avid ACS Monitor which can be used to verify the status and configuration details of the MediaCentral Platform Services system.



avid.acs.attributes

[v0] Storage and Retrieval of Attributes and Attribute Trees

global 0

#	Type	Host	PID	BAL	Build	Platform ID	Environment ID	Scope
1	Service	wavd-doc01	14841	node.js 3.6.2	3.5.2_1_g8429f99-1.x86_64	unknown	unknown	zone
	Gateway	wavd-doc01	14614	java 3.6.3.9_g0573d0f	3.6.3_9_g0573d0f-1.x86_64	unknown	unknown	

[v3] Storage and Retrieval of Attributes

global 0

#	Type	Host	PID	BAL	Build	Platform ID	Environment ID	Scope
1	Service	wavd-doc01	14841	node.js 3.6.2	3.5.2_1_g8429f99-1.x86_64	unknown	unknown	zone
	Gateway	wavd-doc01	14614	java 3.6.3.9_g0573d0f	3.6.3_9_g0573d0f-1.x86_64	unknown	unknown	

avid.acs.federation

[v3] Federating and Un-Federating w/ Other ICS Zones

global 2

#	Type	Host	PID	BAL	Build	Platform ID	Environment ID	Scope
1	Service	wavd-doc01	14977	node.js 3.6.2	3.5.2_3_g3db418c-1.x86_64	unknown	unknown	zone
	Gateway	wavd-doc01	14614	java 3.6.3.9_g0573d0f	3.6.3_9_g0573d0f-1.x86_64	unknown	unknown	

avid.acs.gateway

[v3] Avid ACS Gateway Service.

global 0

#	Type	Host	PID	BAL	Build	Platform ID	Environment ID	Scope
1	Service Gateway	wavd-doc01	14614	java 3.6.3.9_g0573d0f	3.6.3_9_g0573d0f-1.x86_64	unknown	unknown unknown	zone

The ACS Monitor is a powerful tool capable of not only viewing, but also modifying the MediaCentral Platform Services environment. Modifying services through this tool could result in service or system failures.

Accessing the Avid ACS Monitor Tool

The ACS Monitor is not enabled by default and must be started manually.

To enable and access the ACS Monitor:

1. Log in to the MCS server as the Linux ‘root’ user. If you have a clustered configuration, log into the master node.
2. Start the avid-acs-monitor service:

   ```
   service avid-acs-monitor start
   ```

3. Open a web browser and enter the following address to access the Avid ACS Monitor:

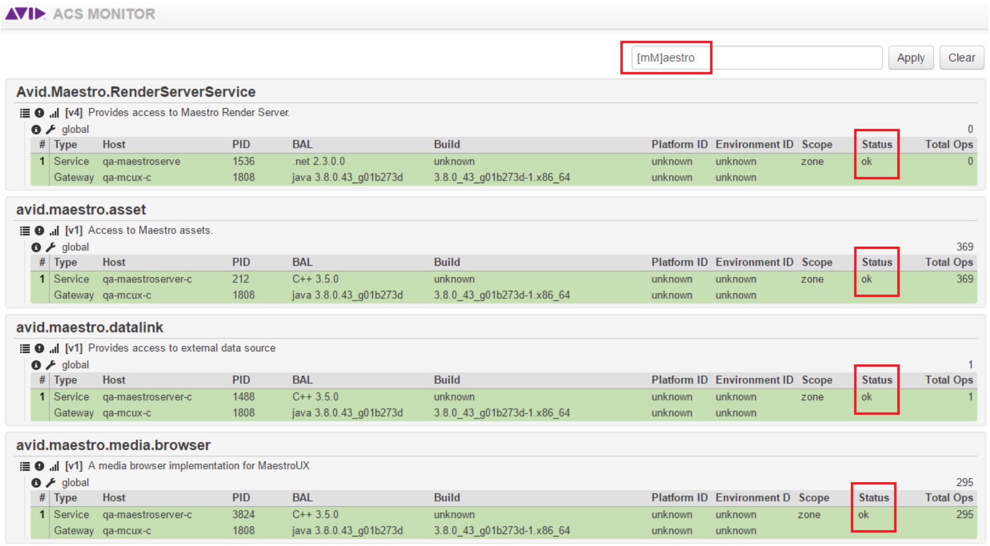
   http://*<server>*:8000

   Where <*server*> is the host name or IP address of your MediaCentral server or cluster master node.

   The Avid ACS Monitor page appears, allowing you to review the system configuration.

If you do not see the list of attributes on the left side of the page, refresh the browser page.

4. Enter “[mM]aestro” (without the quotes) in the search field at the top of the page and click Apply to find the Maestro services.



Avid.Maestro.RenderServerService

[v4] Provides access to Maestro Render Server.

global 0

#	Type	Host	PID	BAL	Build	Platform ID	Environment ID	Scope	Status	Total Ops
1	Service	qa-maestroserve	1536	.net 2.3.0.0	unknown	unknown	unknown	zone	ok	0
	Gateway	qa-mcux-c	1808	java 3.8.0.43_g01b273d	3.8.0_43_g01b273d-1.x86_64	unknown	unknown			

avid.maestro.asset

[v1] Access to Maestro assets.

global 369

#	Type	Host	PID	BAL	Build	Platform ID	Environment ID	Scope	Status	Total Ops
1	Service	qa-maestroserver-c	212	C++ 3.5.0	unknown	unknown	unknown	zone	ok	369
	Gateway	qa-mcux-c	1808	java 3.8.0.43_g01b273d	3.8.0_43_g01b273d-1.x86_64	unknown	unknown			

avid.maestro.datalink

[v1] Provides access to external data source

global 1

#	Type	Host	PID	BAL	Build	Platform ID	Environment ID	Scope	Status	Total Ops
1	Service	qa-maestroserver-c	1488	C++ 3.5.0	unknown	unknown	unknown	zone	ok	1
	Gateway	qa-mcux-c	1808	java 3.8.0.43_g01b273d	3.8.0_43_g01b273d-1.x86_64	unknown	unknown			

avid.maestro.media.browser

[v1] A media browser implementation for MaestroUX

global 295

#	Type	Host	PID	BAL	Build	Platform ID	Environment D	Scope	Status	Total Ops
1	Service	qa-maestroserver-c	3824	C++ 3.5.0	unknown	unknown	unknown	zone	ok	295
	Gateway	qa-mcux-c	1808	java 3.8.0.43_g01b273d	3.8.0_43_g01b273d-1.x86_64	unknown	unknown			

Verify that the status column for each of the services reports a status of “ok”.

5. Once you have verified the status of all services, close the ACS monitor and stop the avid-acs-monitor service on the MCS server:

```
service avid-acs-monitor stop
```

Configuring the Maestro Render Server

Once installed, the Maestro Render Server must be configured to specify a rendering profile and a rendering channel.

To configure the render settings:

1. Launch the Maestro Render Server software at:

   C:\Orad\MaestroRenderServer64\RenderManager.exe

2. At the Login window, enter the following information:

   - Login and Password: Enter the user and password that can access the MaestroRenderServer database.

     Example: sa

   - Server name: Enter the host name of the server running the MSSQL Maestro Render Server database as well as the instance name of the database.

     Example: wavd-maestro01\maestro

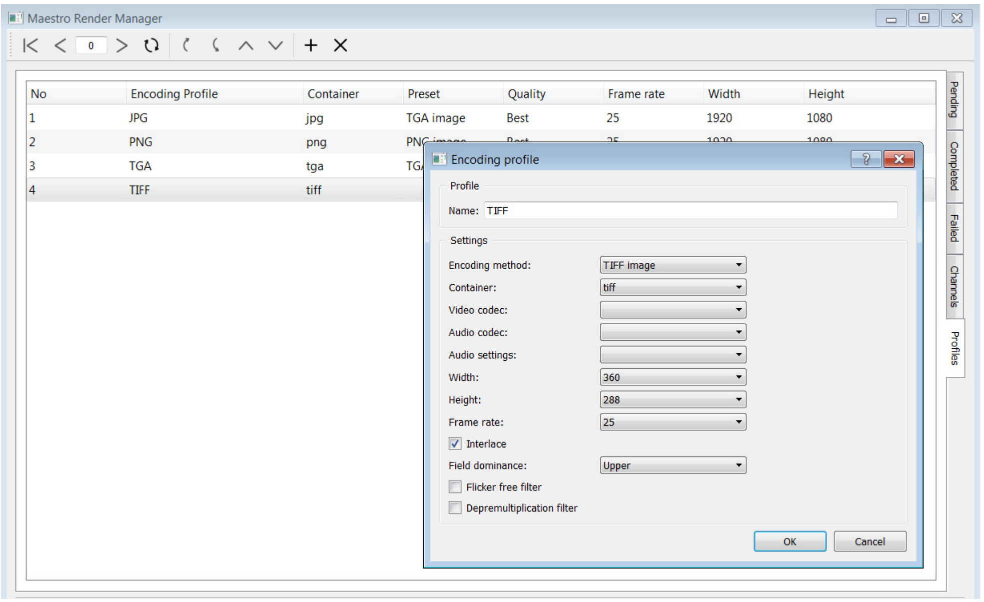
   - Database name: Enter the name of the Masestro Render Server database

     Example: MaestroRenderServer (default)

   - Server type: Select MSSQL database

   - Authentication: Select SQL ServerAuthentication

3. Click the Login button to log in and open the Maestro Render Server Manager.
4. Define a rendering profile to specify the format and resolution of the images to be processed by the Render Server. Begin by clicking on the Profiles tab.
5. Double-click on one of the predefined profiles or define a custom profile by pressing the "+" button in the tool bar.



No	Encoding Profile	Container	Preset	Quality	Frame rate	Width	Height
1	JPG	jpg	TGA image	Best	25	1920	1080
2	PNG	png	PNG image	Best	25	1920	1080
3	TGA	tga	TG				
4	TIFF	tiff					

Encoding profile

Profile

Name: TIFF

Settings

Encoding method: TIFF image

Container: tiff

Video codec:

Audio codec:

Audio settings:

Width: 360

Height: 288

Frame rate: 25

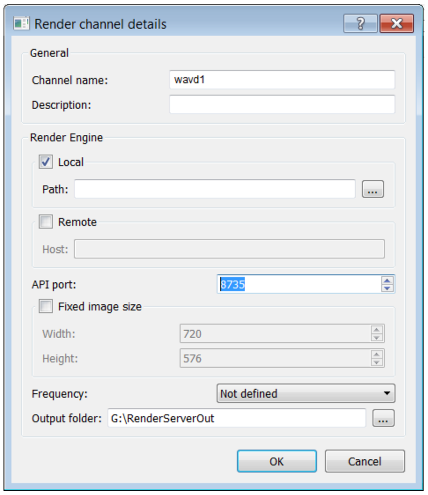
☑ Interlace

Field dominance: Upper

☐ Flicker free filter

☐ Depremultiplication filter

6. Adjust the configuration of the profile. The following lists a few recommended settings:
   - Encoding method: TIFF recommended
   - Container: TIFF recommended
   - Do not configure the fields in such a way that the final resolution is too high. A high resolution image slows down the preview generation process.
7. Once the profile is complete, click OK.
8. Next, you must configure a rendering channel. Begin by clicking on the Channels tab.
9. Click the "+" button in the tool bar to create a new Render channel.



Render channel details

General

Channel name: wavd1

Description:

Render Engine

☑ Local

Path:

☐ Remote

Host:

API port: 8735

☐ Fixed image size

Width: 720

Height: 576

Frequency: Not defined

Output folder: G:\RenderServerOut

10. Adjust the configuration of the profile.:

    a. Channel name: Enter the name of the Render channel.

       The Channel name must not contain spaces.

    b. Under the Render Engine category, verify that the Local check box is selected.

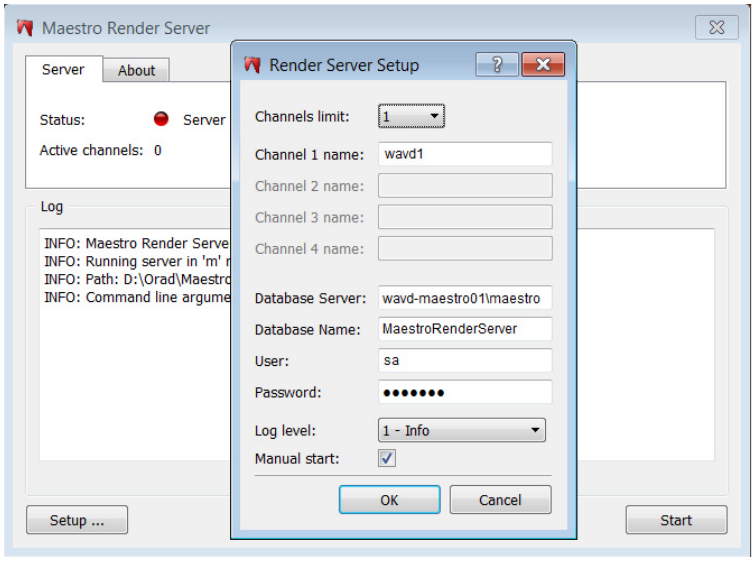
       This document instructs you to install the Maestro Render Server and the RenderServerService on the same server. Selecting "Local" assumes this was completed.

    c. Verify or configure the Output folder. The default value configured for this field is "RenderServerOut". However, an alternate path can be specified if preferred.

11. Click OK to save the profile.

12. Finally, you must start the Maestro Render Server application.

    Click the Setup button to access the Render Server Setup window.



Status: ● Server

Active channels: 0

```
INFO: Maestro Render Serve
INFO: Running server in 'm' r
INFO: Path: D:\Orad\Maestro
INFO: Command line argume
```

Channels limit: 1

Channel 1 name: wavd1

Channel 2 name:

Channel 3 name:

Channel 4 name:

Database Server: wavd-maestro01\maestro

Database Name: MaestroRenderServer

User: sa

Password: •••••••

Log level: 1 - Info

Manual start: ☑

13. Set the "Channels limit" menu to 1.

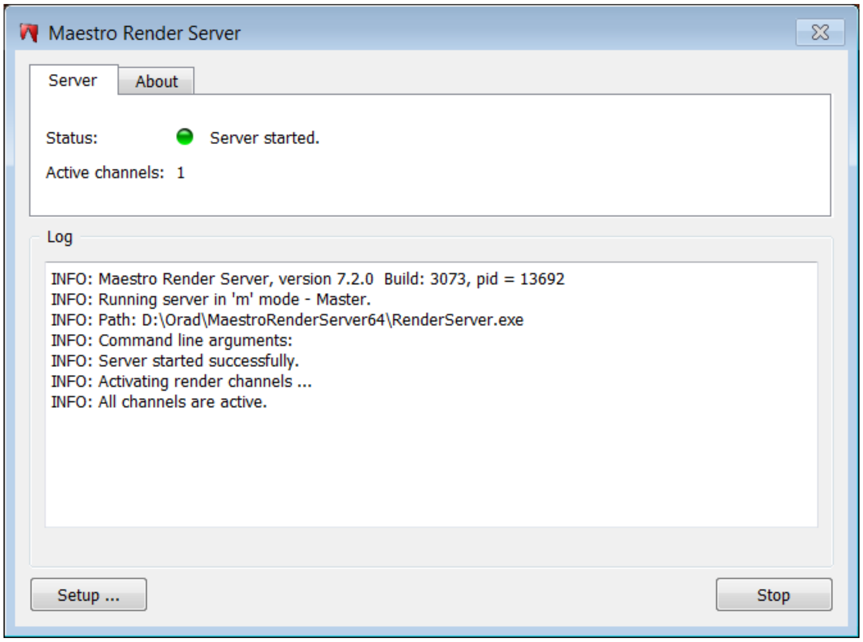
    The "Channel 1 name" should already have been configured during the Render channel setup process. If the channel does not have a name, assign one at this time.

14. Click OK to save the Render Server Setup window.

15. Click the Start button to start the server.

    After a few moments, you should see a "All channels are active" message indicating that the channel creation process was successful.

    The following image depicts the completed configuration:



Status: Server started.

Active channels: 1

```
INFO: Maestro Render Server, version 7.2.0  Build: 3073, pid = 13692
INFO: Running server in 'm' mode - Master.
INFO: Path: D:\Orad\MaestroRenderServer64\RenderServer.exe
INFO: Command line arguments:
INFO: Server started successfully.
INFO: Activating render channels ...
INFO: All channels are active.
```

Installing the Plug-Ins on the MCS Server

Installing the Maestro UX plug-in on the MediaCentral Platform Services server involves two simple steps:

- Preparing the Software Package
- Installing the Plug-Ins on the MCS Server

Preparing the Software Package

The Maestro UX plug-in software includes three .rpm files that need to be installed on the MCS server:

- `maestro-ux-<`*`version`*`>.noarch.rpm`
- `maestro-ux-media-browser-<`*`version`*`>.noarch.rpm`
- `MaestroUX-<`*`version`*`>.x86_64.rpm`

Before you can start the installation, you must obtain the .rpm files and copy them to your MediaCentral server. These packages can be found in the GraphicsSuite_<*version*>.zip file discussed earlier in this chapter. If you have a cluster configuration, complete the steps below on the master and slave nodes only.

To prepare the software package:

1. Ensure that you have obtained and copied the Maestro UX plug-in software to the MCS server.

   For more information, see “Copying Software to the MCS Server” on page 238.

2. Navigate to the directory where the installer files have been copied. Example:

   ```
   cd /media/installers
   ```

Installing the Plug-Ins on the MCS Server

If you are running a cluster, complete the process below on the master and slave nodes only. Complete the process on the slave node first and then repeat the process on the master node.

To install the Maestro plug-in software:

1. If you have not already done so, navigate to the directory containing the Maestro UX installer. Example:

   ```
   cd /media/installers
   ```

2. Three .rpm files are required to be installed on the MCS server. Install the files with the following commands:

   ```
   rpm -ivh maestro-ux-<version>.noarch.rpm
   ```

   ```
   rpm -ivh maestro-ux-media-browser-<version>.noarch.rpm
   ```

   ```
   rpm -ivh MaestroUX-<version>.x86_64.rpm
   ```

3. Mount the shared location where Maestro Render Server is storing rendered images for playback through MediaCentral UX.

   a. Create a mount point on the MCS server for the shared folder:

   ```
   mkdir /Control_Data
   ```

   b. Edit the /etc/fstab file to automate the mapping shared folder on startup:

   ```
   vi /etc/fstab
   ```

   c. Add an entry at the end of the file:

   ```
   //<shared_folder_host>//<shared_folder_name> /Control_Data cifs
   ro,user=<user_name>,passwd=<user_pass>,iocharset=utf8 0 0
   ```

   Where the following variables are used:

   - *<shared_folder_host>* is the IP address or host name of the server hosting the Maestro Render Server.
   - *<shared_folder_name>* is the name of the shared folder on Render Server (RenderServerOut by default).
   - *<user_name>* is the name of a Windows user on the Maestro system that has access to this share.
   - *<user_pass>* is the password for the above user.

   Below is an example of the completed line:

   ```
   //192.168.10.99/Data /Control_Data cifs
   ro,user=Maestro,passwd=Avid123,iocharset=utf8 0 0
   ```

   d. Save and exit the vi session. Press <ESC> and type: **:wq**

   e. Mount the volume:

   ```
   mount /Control_Data
   ```

4. Update the avid-acs-gateway configuration file with the IP address of the Maestro server.

   For more information, see "Configuring Access for External Systems" on page 78.

   a. Using the Linux text editor, *vi*, open the configuration file for editing:

   ```
   vi /etc/sysconfig/avid-acs-gateway
   ```

b. Locate the following line in the configuration file:

```
#export ACS_SECURITY_FULL_TRUST_IPV4_MASK_LIST="127.0.0.1/25;"
```

c. Activate (uncomment) this line by removing the “#” in front of it.

d. Add the IP address of the Maestro server to this line, followed by a semicolon:

```
export ACS_SECURITY_FULL_TRUST_IPV4_MASK_LIST=”127.0.0.1/25;<ip>;”
```

In the following example, 192.168.10.99 is the IP address of the server

```
#export ACS_SECURITY_FULL_TRUST_IPV4_MASK_LIST="127.0.0.1/
25;192.168.10.99;"
```

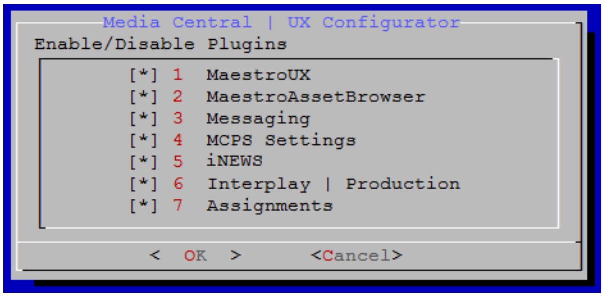
Do not remove the 127.0.0.1/25 address from this line. This address is required for MediaCentral Platform Services to operate.

e. Save and exit the vi session. Press <ESC> and type: **`:wq`**

5. Use the MediaCentral Configurator tool to enable the Maestro plug-ins. Start the Configurator by typing the following at the Linux prompt:

   `/opt/avid/avid-interplay-central/configurator`

   The configuration UI appears.



```
Media Central | UX Configurator
Enable/Disable Plugins
        [*] 1  MaestroUX
        [*] 2  MaestroAssetBrowser
        [*] 3  Messaging
        [*] 4  MCPS Settings
        [*] 5  iNEWS
        [*] 6  Interplay | Production
        [*] 7  Assignments

      <  OK  >        <Cancel>
```

6. Enable the MaestroUX and MaestroAssetBrowser options in the Configurator and select OK.

   Use the Up and Down arrow keys to move between the options, Left and Right arrow keys to move between OK and Cancel, SPACEBAR to toggle the asterisks, and press Enter to confirm.

   - Asterisk = enabled
   - No Asterisk = disabled

   For more information, see “Working with the MediaCentral UX Configurator” on page 259.

Configure users

For each MediaCentral user that will require access to Maestro UX pane, a corresponding user should be created with Maestro Admin tool. If the user is not recognized by the Maestro server, the user will not see anything in Maestro asset list window.

For details instructions on creating users, see the “Access and Permissions” chapter of the *Avid Maestro Users Guide* v7.2 or later.

Configuring the MediaCentral UX System Settings

With the software installed on the Maestro and MCS server, the final step in the process involves configuring the new Maestro System Setting within MediaCentral UX.

To configure the Maestro system setting:

1. Sign in to MediaCentral UX as a user with administrator-level access.

   For details on this process, see "Signing into MediaCentral UX" on page 92.

2. Select "System Settings" from the Layout selector in the top-right corner of the interface. This layout only appears if you are logged in as a user with administrator rights.
3. In the Settings pane, select Maestro.
4. Configure the MOS options:
   - MOS Object Timebase: Select either NTSC or PAL
   - MOS ID: This is the ID of the Orad MOS Gateway.
5. Configure the Render Server options:
   - Output folder: Enter the path of the share on the MCS server for the output folder.

     Example: /Control_Data/RenderServerOut

   - Render server profile: Enter the name of the render profile you altered or created during the process for "Configuring the Maestro Render Server" on page 192.

     Example: TIFF

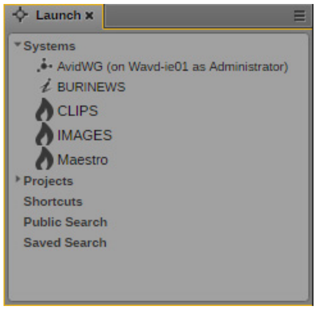
6. Click Apply to save your changes.
7. Once the System Settings have been applied, sign out of MediaCentral UX
8. Restart the avid-interplay-central service to enable the changes.
   - If running a single server configuration:

     ```
     service avid-interplay-central restart
     ```

   - If running a clustered configuration, issue the following command on any node in the cluster:

     ```
     crm resource restart AvidIPC
     ```

9. Sign back in to MediaCentral UX as any user. Icons representing the Maestro Asset database (Maestro) and filesystem assets (CLIPS and IMAGES) should appear in the Launch pane of the MediaCentral UX user interface.



Additionally, a new "Maestro Browser" pane that enables users to edit and create rendered previews of Maestro assets should be available from the Panes menu.

Upgrading Maestro UX

The process for upgrading the Maestro UX software follows one of two paths, depending on the version of software currently installed on your servers. Complete one of the following processes as applicable to your installation:

- "Upgrading from MediaCentral Platform Services v2.7.x" on page 199
- "Upgrading from MediaCentral Platform Services v2.8.0 or later" on page 200

MediaCentral Platform Services v2.7.x and v2.8.x do not support installing the Maestro UX software in a clustered configuration. Support for clusters was added in MCS v2.9.0. Therefore the steps to upgrade Maestro UX for this release only apply to single server configurations.

The Maestro UX upgrade process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and sign off during the upgrade.

Upgrading from MediaCentral Platform Services v2.7.x

The process for upgrading the Maestro UX software consists of two parts:

- Upgrading the software on the MediaCentral Platform Services server
- Upgrading the software on the Maestro server

Complete the two processes in this section to upgrade the Maestro UX software.

To upgrade the Maestro UX software on the MCS server:

1. Log into the MCS server (at the Linux prompt) as the root user.
2. Uninstall the currently installed Maestro packages:

   ```
   rpm -e maestro-ux-<version>.noarch.rpm
   ```

   ```
   rpm -e MaestroUX-<version>.x86_64.rpm
   ```

3. Copy the new Maestro software packages to the MCS server.

   For details, see "Preparing the Software Package" on page 195.

4. If you have not already done so, navigate to the directory containing the Maestro UX installer. Example:

   ```
   cd /media/installers
   ```

5. Three .rpm files are required to be installed on the MCS server. Install the files with the following commands:

   ```
   rpm -ivh maestro-ux-<version>.noarch.rpm
   ```

   ```
   rpm -ivh maestro-ux-media-browser-<version>.noarch.rpm
   ```

   ```
   rpm -ivh MaestroUX-<version>.x86_64.rpm
   ```

6. Launch the MediaCentral Configurator tool to enable the Maestro plug-ins:

   ```
   /opt/avid/avid-interplay-central/configurator
   ```

   Enable the Maestro plug-ins and select OK.

   For more information, see "Working with the MediaCentral UX Configurator" on page 259.

To upgrade the Maestro UX software on the Maestro server:

1. Sign -in to the Maestro server as a user with administrator-level access.
2. The Graphics Suite installation package includes the software required to enable workflows between Maestro and MediaCentral Platform Services. Copy the installer to the desktop of the Maestro server.
3. Unzip the GraphicsSuite_<*version*>.zip file to its own folder.
4. Stop the Data Link Service and the Maestro Bus Service through the Windows Computer Management utility.
5. Uninstall the Data Link Service and Maestro Bus Service using the Windows "Programs and Features" Control Panel.
6. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Bus Services installer "MaestroBusServices_<*version_build*>.exe" to reinstall the software.

   For details, see "Installing the Maestro Bus Services" on page 188.
7. Enable the services through the Maestro Monitor application.

   For details, see "Enabling the Services" on page 190.
8. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Render Server installer "Maestro64_<*version_build*>.exe" to upgrade the software.

   For details, see "Installing the Maestro Render Server" on page 186.
9. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Render Server Service installer "RenderServerService_<*version_build*>.exe" to upgrade the software.

   For details, see "Installing the Render Server Service" on page 187.

Upgrading from MediaCentral Platform Services v2.8.0 or later

The process for upgrading the Maestro UX software consists of two parts:

- Upgrading the software on the MediaCentral Platform Services server
- Upgrading the software on the Maestro server

Complete the two processes in this section to upgrade the Maestro UX software.

To upgrade the Maestro UX software on the MCS server:

1. Log into the MCS server (at the Linux prompt) as the root user.
2. Copy the new Maestro software packages to the MCS server.

   For details, see "Preparing the Software Package" on page 195.
3. If you have not already done so, navigate to the directory containing the Maestro UX installer. Example:

   ```
   cd /media/installers
   ```
4. Three .rpm files are required to be installed on the MCS server. Upgrade the files with the following commands:

   ```
   rpm -Uvh maestro-ux-<version>.noarch.rpm
   ```

   ```
   rpm -Uvh maestro-ux-media-browser-<version>.noarch.rpm
   ```

   ```
   rpm -Uvh MaestroUX-<version>.x86_64.rpm
   ```

5. Launch the MediaCentral Configurator tool to enable the Maestro plug-ins:

   ```
   /opt/avid/avid-interplay-central/configurator
   ```

   Enable the Maestro plug-ins and select OK.

   For more information, see "Working with the MediaCentral UX Configurator" on page 259.

To upgrade the Maestro UX software on the Maestro server:

1. Sign -in to the Maestro server as a user with administrator-level access.
2. The Graphics Suite installation package includes the software required to enable workflows between Maestro and MediaCentral Platform Services. Copy the installer to the desktop of the Maestro server.
3. Unzip the GraphicsSuite_<*version*>.zip file to its own folder.
4. Open the Maestro Monitor application:
   - From the Windows Start menu at:

     Start > All Programs > Orad > MaestroMonitor
   - Through the executable in the system file structure:

     C:\Orad\MaestroBusServices\MaestroMonitor.exe

   The Monitor tool opens, showing the services and their current status.
5. Click the Stop button in the lower-right corner of the window to stop all services.
6. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Bus Services installer "MaestroBusServices_<*version_build*>.exe" to upgrade the software.
7. Once the Maestro Bus Services have been upgraded, open the Maestro Monitor and restart all services.
8. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Render Server installer "Maestro64_<*version_build*>.exe" to upgrade the software.

   For details, see "Installing the Maestro Render Server" on page 186.
9. Open the GraphicsSuite_<*version*> folder and double-click the Maestro Render Server Service installer "RenderServerService_<*version_build*>.exe" to upgrade the software.

   For details, see "Installing the Render Server Service" on page 187.

Uninstalling Maestro UX

In the event that you need to disable the functionality added by the Maestro UX, use the following processes to uninstall the software on the MediaCentral and Maestro servers.

The Maestro UX uninstall process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and sign off during the upgrade.

Uninstalling Maestro UX from MediaCentral Platform Services

The process to uninstall the Maestro UX software on a single-server and a cluster are similar. In a cluster configuration, the Maestro UX software is installed on the Corosync Master and Slave nodes. When uninstalling the software in a cluster, complete the process below on the slave node first. Once complete, repeat the process on the master node.

To uninstall the Maestro UX software on the MCS server:

1. Log into the MCS server (at the Linux prompt) as the root user.
2. Launch the MediaCentral Configurator tool to disable the Maestro plug-ins:

   ```
   /opt/avid/avid-interplay-central/configurator
   ```

   Deselect the Maestro plug-ins from the list of features and select OK.

   For more information, see "Working with the MediaCentral UX Configurator" on page 259.
3. Uninstall the currently installed Maestro packages:

   ```
   rpm -e maestro-ux-<version>.noarch.rpm
   ```

   ```
   rpm -e maestro-ux-media-browser-<version>.noarch.rpm
   ```

   ```
   rpm -e MaestroUX-<version>.x86_64.rpm
   ```
4. If running a cluster configuration, repeat the steps above on the cluster master node.
5. Proceed to "Uninstalling Maestro UX on the Maestro Server" on page 202 to complete the removal process.

Uninstalling Maestro UX on the Maestro Server

To uninstall the Maestro UX software on the Maestro server:

1. Sign -in to the Maestro server as a user with administrator-level access.
2. Open the Maestro Monitor application:
   - From the Windows Start menu at:

     Start > All Programs > Orad > MaestroMonitor
   - Through the executable in the system file structure:

     C:\Orad\MaestroBusServices\MaestroMonitor.exe

   The Monitor tool opens, showing the services and their current status.
3. Click the Stop button in the lower-right corner of the window to stop all services.
4. Use the Windows "Programs and Features" Control Panel to uninstall the Maestro Render Server, the Render Server Service, and the Maestro Bus Services.

Additional Information

This section includes additional details for altering the Maestro UX configuration.

Altering the Configuration

If required, system administrators can alter the settings configured during the Maestro Bus Services installation process. These processes enable administrators to change settings without needing to reinstall the services. The process for altering the ACS Gateway settings might be useful if a change has been made to the MCS configuration - such as an upgrade from a single-server environment to a cluster - or if network port changes are required.

To alter the Maestro file paths:

1. Log in to the Maestro server as a user with administrator-level access.
2. Use the Maestro Monitor to stop the Maestro services.

   For more information on the Maestro Monitor, see "Enabling the Services" on page 190.
3. Navigate to the location of the "SystemSettings.ini" file:

   C:\Orad\MaestroBusServices\
4. Double-click on the file to begin editing the values.
5. Edit any required values and save the file.
6. Once the edits are complete, restart the services through the Maestro Monitor.

To alter the ACS_GATEWAY settings:

1. Log in to the Maestro server as a user with administrator-level access.
2. Use the Maestro Monitor to stop the Maestro services.

   For more information on the Maestro Monitor, see "Enabling the Services" on page 190.
3. Open the Windows command prompt utility by typing "cmd" (without the quotes) in the Run option of the Windows Start menu.
4. In the Command window, enter the following to verify the current ACS_GATEWAY settings:

   `set acs`

   Results similar to the following should appear:

   ```
   C:\Users\Administrator> set acs
   ACS_GATEWAY_HOST=192.168.10.50
   ACS_GATEWAY_PORT=9900
   ```
5. Once the edits are complete, you must reboot the server to enable the changes.

11 Assignments Pane

Chapter Overview

The purpose of this chapter is to guide you through the installation and configuration of the Assignments pane introduced with MediaCentral Platform Services v2.9.

The following table describes the topics that are covered in this chapter:

Step	Task	Time Est.
1	Preparing the Software Package	5 min
	Process for copying and unzipping the installer.	
2	Installing the Assignments Pane on a Single Server	5 min
	Process for installing the Assignments pane on a single MCS server.	
3	Installing the Assignments Pane in a Cluster	15 min
	Process for installing the Assignments pane in an MCS cluster.	
4	Configuring the Assignments Pane	5 min
	Once the software is installed, the MediaCentral UX System Settings must be updated.	
- -	Uninstalling the Assignments Pane	15 min
	Process for removing the Assignments pane software from the MediaCentral server.	
- -	Backing Up and Restoring the Assignments Database	5 min
	Process for backing-up and restoring the assignments data stored in the MongoDB database.	

This feature enables new collaborative workflows in MediaCentral UX where an “Assignment” becomes the core idea around which all elements are linked. Resources in the form of users, media assets, iNEWS stories, notes, and more are attached to the Assignment and tasks can be issued to specific users based on the requirements of the job and the user’s skill set.

The Assignments pane is not included with a standard MCS installation and must be installed separately.

The installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and sign off during the installation or upgrade procedures.

If integrating with Avid iNEWS, the iNEWS servers must be running v5.x or later to use the Assignments pane.

For more information on this feature, see the “The Assignments Pane” chapter of the *Avid MediaCentral | UX User’s Guide*.

Preparing the Software Package

Before you can start the installation, you must obtain the Assignments pane software and copy it to your MediaCentral server(s). If you have a cluster configuration, complete steps below on the master and slave nodes only.

To prepare the software package:

1. Ensure that you have obtained and copied the software to the MCS server(s). If you have not completed these tasks, see "Obtaining the Software" on page 21 and "Copying Software to the MCS Server" on page 238 for instructions.
2. Navigate to the directory where the installer has been copied. Example:

   ```
   cd /media/installers
   ```

3. If necessary, unzip the installer:

   ```
   unzip MediaCentral_Assignments_<x.x.x>_Linux.zip
   ```

4. Navigate to the newly created directory:

   ```
   cd MediaCentral_Assignments_<x.x.x>_<build>_Linux
   ```

Installing the Assignments Pane on a Single Server

This section details the steps required to install the Assignments pane on a single-server.

To install the Assignments pane:

1. If you have not already done so, navigate to the directory containing the installation script:

   ```
   cd /<path>
   ```

2. Run the Assignments pane installation script:

   ```
   ./install.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   The process should complete with messages similar to the following, indicating a successful installation:

   ```
   Complete!
   Starting avid-interplay-central
   avid-interplay-central process has been started.
   Wait for avid-interplay-central web interface...
   Avid Interplay Central has been started successfully (15 seconds)    [ OK ]
   ```

3. Once the software is installed, proceed to "Configuring the Assignments Pane" on page 208 to update the MediaCentral UX System Settings.

Installing the Assignments Pane in a Cluster

In a cluster deployment, the Assignments pane is installed on the master and slave nodes only.

The cluster installation process involves the following steps:

- Preparing the Software Package
- Verifying Prerequisites
- Installing the Assignments Pane
- Checking on the Cluster Status

Verifying Prerequisites

Prior to installing the Assignments pane, verify the following:

- MCS is installed and configured on all servers in the cluster.
- All cluster resources should be online and free of errors.

  Use “crm_mon -f” to verify the cluster status.

Unlike installations such as the Closed Captioning Service or the MAM Connector, all cluster nodes must be online prior to installing the Assignments pane software. The Assignments pane integrates with the MongoDB (non-sharded) database located on the master and slave nodes and all related services must be active during the installation process.

Installing the Assignments Pane

Complete the following process on the cluster master and slave nodes. Install the software on the slave node first, followed by the master node.

To install the Assignments pane:

1. If you have not already done so, navigate to the directory containing the installation script:

   ```
   cd /<path>
   ```

2. Run the Assignments pane installation script:

   ```
   ./install.sh
   ```

   The period-slash “./” in this command tells Linux to look for the script in the current directory.

   The process should complete with a message similar to the following, indicating a successful installation:

   ```
   Complete!
   ```

3. Repeat steps 1 and 2 on the master node.

The process should finish with a similar “Complete!” message, but will also include information related to updates for the MongoDB database and a restart of the AvidIPC resource similar to the following:

```
Complete!

Set 'AvidIPC' option: id=AvidIPC-meta_attributes-target-role set=AvidIPC-
meta_attributes name=target-role=stopped

Waiting for 1 resources to stop:

 * AvidIPC

Deleted 'AvidIPC' option: id=AvidIPC-meta_attributes-target-role
name=target-role

Waiting for 1 resources to start again:

 * AvidIPC
```

Checking on the Cluster Status

With the Assignments pane installed, verify that all cluster resources are running and that the Cluster Resource Monitor is free of errors.

To verify the cluster status:

1. Use the Cluster Resource Monitor to verify the status of the cluster:

   ```
   crm_mon -f
   ```

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Review the fail-counts for the cluster resources.

2. If there are fail-counts listed, run the Cluster Resource Manager cleanup command to reset them:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   <*rsc*> is the resource name of interest: AvidIPC, pgsqlDB (or another)

   <*node*> (optional) is the node of interest

If you receive an “object/attribute does not exist” error message, it indicates the resource is active on more than one node. Repeat the command using the “everywhere” form of the resource.

   For example, to reset the fail-count for AvidAll resource, issue the following command:

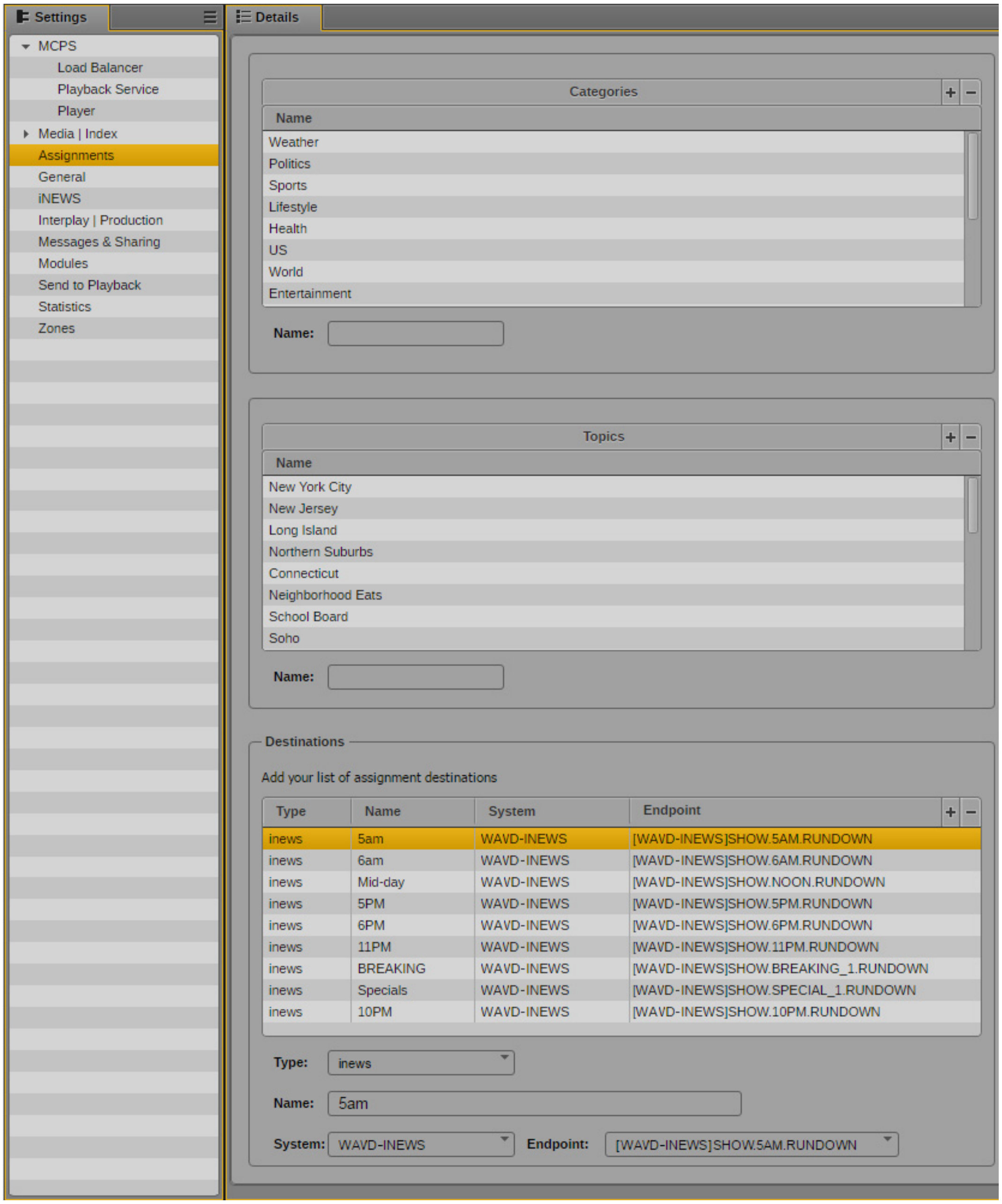
   ```
   crm resource cleanup AvidAllEverywhere
   ```

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

3. Once the software is installed, proceed to “Configuring the Assignments Pane” on page 208 to update the MediaCentral UX System Settings.

Configuring the Assignments Pane

The installation of the Assignments pane adds a new line item to the MediaCentral UX System Settings called “Assignments”.



Categories

Name
Weather
Politics
Sports
Lifestyle
Health
US
World
Entertainment

Name:

Topics

Name
New York City
New Jersey
Long Island
Northern Suburbs
Connecticut
Neighborhood Eats
School Board
Soho

Name:

Destinations

Add your list of assignment destinations

Type	Name	System	Endpoint
inews	5am	WAVD-INEWS	[WAVD-INEWS]SHOW.5AM.RUNDOWN
inews	6am	WAVD-INEWS	[WAVD-INEWS]SHOW.6AM.RUNDOWN
inews	Mid-day	WAVD-INEWS	[WAVD-INEWS]SHOW.NOON.RUNDOWN
inews	5PM	WAVD-INEWS	[WAVD-INEWS]SHOW.5PM.RUNDOWN
inews	6PM	WAVD-INEWS	[WAVD-INEWS]SHOW.6PM.RUNDOWN
inews	11PM	WAVD-INEWS	[WAVD-INEWS]SHOW.11PM.RUNDOWN
inews	BREAKING	WAVD-INEWS	[WAVD-INEWS]SHOW.BREAKING_1.RUNDOWN
inews	Specials	WAVD-INEWS	[WAVD-INEWS]SHOW.SPECIAL_1.RUNDOWN
inews	10PM	WAVD-INEWS	[WAVD-INEWS]SHOW.10PM.RUNDOWN

Type: inews

Name: 5am

System: WAVD-INEWS Endpoint: [WAVD-INEWS]SHOW.5AM.RUNDOWN

Prior to working with the Assignments pane, you should define the Categories, Topics, and Definitions to be used in the workflow. For more information, see “Configuring the Assignments Pane” in the *Avid MediaCentral UX Users Guide*.

Uninstalling the Assignments Pane

In the event that you need to disable the functionality added by the Assignments pane, use one of the following processes to uninstall the software.

This process will disconnect any users currently working on the system. Make sure all users save their work prior to completing this process.

Uninstalling the Assignments Pane on a Single Server

To uninstall the software on a single server:

1. Navigate to the directory containing the Assignments pane installation files:

   ```
   cd /<path>
   ```

2. Run the Assignments pane uninstall script:

   ```
   ./uninstall.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   The software is uninstalled and the avid-interplay-central service is restarted.

Uninstalling the Assignments Pane on a Cluster

To uninstall the Assignments pane on a cluster:

1. Verify the current Master, Slave and load balancing nodes. For more information, see "Identifying the Master, Slave and Load-Balancing Nodes" on page 268.
2. Starting with the master node, navigate to the directory containing the Assignments pane installation files:

   ```
   cd /<path>
   ```

3. Run the Assignments pane uninstall script:

   ```
   ./uninstall.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

4. Repeat steps 2 and 3 on the slave node.
5. Use the Cluster Resource Monitor to verify the status of the cluster:

   ```
   crm_mon -f
   ```

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Verify that the AvidIPC resource is online on the master node.
   - Review the fail-counts for the cluster resources.

6. If there are fail-counts listed, run the Cluster Resource Manager cleanup command to reset them:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   `<rsc>` is the resource name of interest: AvidIPC, pgsqlDB (or another)

   `<node>` (optional) is the node of interest

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the "everywhere" form of the resource.

For example, to reset the fail-count for AvidAll resource, issue the following command:

```
crm resource cleanup AvidAllEverywhere
```

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

Backing Up and Restoring the Assignments Database

If desired, users can manually back up and restore the information stored in the non-sharded MongoDB database. The information below details how to complete those processes.

To back up the assignments database:

Run the following command to create a backup of the database:

```
/opt/avid/bin/avid-db-assignment-dump
```

Backups of the database are created in the `/var/lib/avid/db/dumps` directory and are named similar to the following:

```
assignment-20161122_024307Z.mongo.tar.gz
```

To restore the assignments database:

1. The restore command assumes that the backup file is located at `/var/lib/avid/db/dumps`. If it is not, you must first copy the backup to this directory:

   ```
   cp /<path>/<filename> /var/lib/avid/db/dumps
   ```

   For example:

   ```
   cp /tmp/assignment-20161122_024307Z.mongo.tar.gz /var/lib/avid/db/dumps
   ```

2. Run the following command to restore a backup copy of the database:

   ```
   /opt/avid/bin/avid-db-assignment-restore <filename_without_extension>
   ```

   For example:

   ```
   /opt/avid/bin/avid-db-assignment-restore assignment-20161122_024307Z.mongo
   ```

   Make sure that you do not include the .tar.gz extension in this command.

   The restore process prints a series of messages to the screen and completes with a “done” statement:

   ```
   2016-11-30T15:23:00.803-0500    finished restoring
   assignment_centric.version (1 document)

   2016-11-30T15:23:00.803-0500    finished restoring
   assignment_centric.assignment (2 documents)

   2016-11-30T15:23:00.803-0500    done

   Mongo Database restored from /var/lib/avid/db/dumps/assignment-
   20161130_174829Z.mongo.tar.gz
   ```

12 MAM Connector

Chapter Overview

The purpose of this chapter is to guide you through the installation of the MAM Connector software.

The following table describes the topics that are covered in this chapter:

Step	Task	Time Est.
1	Preparing the Software Package	5 min
	Process for copying and unzipping the MAM Connector software.	
2	Installing the MAM Connector on a Single Server	5 min
	Process for installing the MAM Connector on a single MCS server.	
3	Installing the MAM Connector in a Cluster	5 min
	Process for installing the MAM Connector on an MCS cluster.	
4	Configuring the MAM Connector	5 min
	Once the MAM Connector has been installed, the MediaCentral UX System Settings must be configured.	
- -	Upgrading the MAM Connector	*varies*
	Process for upgrading from a previous version of the MAM Connector.	
- -	Uninstalling the MAM Connector	*varies*
	In the event that you no longer require Interplay MAM workflows, the MAM Connector software can be easily removed.	

Installed on the MediaCentral Platform Services server(s), the MAM Connector enables Interplay MAM workflows through MediaCentral UX. The MCS server(s) must be fully installed and configured prior to installing the MAM Connector.

The MAM Connector settings allow users to connect to one or more MAM systems. However, each Interplay MAM system can only connect to a single MediaCentral Platform Services environment. In single-zone environments, simultaneously connecting multiple MCS systems to a single Interplay MAM is not supported at this time. If this workflow is required, you must configure the MediaCentral systems in a multi-zone environment.

For MAM Connector compatibility with MCS, refer to the Software Compatibility Matrix on the Avid Knowledge Base.

The MAM Connector installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and sign off during the installation procedure.

Preparing the Software Package

Before you can start the installation, you must obtain the MAM Connector software and copy it to your MediaCentral server(s). If you have a cluster configuration, complete steps below on the master and slave nodes only.

To prepare the software package:

1. Ensure that you have obtained and copied the software to the MCS server(s). If you have not completed these tasks, see "Obtaining the Software" on page 21 and "Copying Software to the MCS Server" on page 238 for instructions.
2. Navigate to the directory where the installer has been copied. Example:

   ```
   cd /media/installers
   ```

3. If necessary, unzip the installer:

   ```
   unzip MediaCentral_MAM_Connector_<version>_Linux.zip
   ```

4. Navigate to the newly created directory:

   ```
   cd MediaCentral_MAM_Connector_<version>_<build>_Linux
   ```

Installing the MAM Connector on a Single Server

This section details the steps required to install the MAM Connector on a single-server.

To install the MAM Connector:

1. If you have not already done so, navigate to the directory containing the installation script:

   ```
   cd /<path>
   ```

2. Run the MAM Connector installation script:

   ```
   ./install.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   The process should complete with information similar to the following:

   ```
   Installed:
     avid-interplay-central-mam.noarch <version>.<build>
     avid-mcux-process-dashboard-pane.noarch <version>.<build>

   Complete!
   ```

3. Further verify the success of the installation using the Linux rpm command:

   ```
   rpm -qa | grep mam
   ```

   The output should include the following line:

   ```
   avid-interplay-central-mam-<version>.<build>.noarch.rpm
   avid-mcux-process-dashboard-pane.noarch <version>.<build>.noarch.rpm
   ```

4. Restart the avid-interplay-central service:

   ```
   service avid-interplay-central restart
   ```

5. Proceed to "Configuring the MAM Connector" on page 215 to update the MediaCentral UX System Settings.

Installing the MAM Connector in a Cluster

In a cluster deployment, the MAM Connector is installed on the master and slave nodes only.

The cluster installation process involves the following steps:

- Preparing the Software Package
- Verifying Prerequisites
- Identifying the Master, Slave, and Load-Balancing Nodes
- Taking the Cluster Offline
- Installing the MAM Connector Software
- Bringing the Cluster Back Online
- Checking on the Cluster Status

Verifying Prerequisites

Prior to installing the MAM Connector, verify the following:

- MCS is installed and configured on all servers in the cluster.
- All cluster resources should be online and free of errors.

  Use "`crm_mon -f`" to verify the cluster status.

Identifying the Master, Slave, and Load-Balancing Nodes

There are three types of nodes in a cluster: master, slave, and load-balancing. The master "owns" multiple resources such as the cluster IP address. The slave assumes the role of master in the event of a fail-over. Additional nodes play a load-balancing role, but can never take on the role of master.

To identify the master, slave, and load-balancing nodes:

1. Verify the current role of each node by logging in to any machine in the cluster as the root user and typing:

   ```
   crm_mon
   ```

2. To identify the master and slave nodes, look for the line containing "Master/Slave Set".

   For example:

   ```
   Master/Slave Set: ms_drbd_postgres [drbd_postgres]
   Masters: [ wavd-mcs01 ]
   Slaves: [ wavd-mcs02 ]
   ```

   In this example, the master node is wavd-mcs01 and the slave node is wavd-mcs02.

3. To identify the load-balancing nodes, look for the line containing "Clone Set":

   ```
   Clone Set: AvidAllEverywhere [AvidAll]
   Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03]
   ```

   In this example, the load-balancing node is wavd-mcs03.

4. Exit crm_mon by pressing CTRL-C on the keyboard.

Taking the Cluster Offline

Prior to installing the MAM Connector, all nodes must be taken offline. To avoid accidental cluster fail-over, make sure to follow the order represented below.

To take the cluster offline:

1. Begin taking the cluster offline by putting the load-balancing nodes into standby mode:

   ```
   crm node standby <node name>
   ```

2. Next, put the slave node into standby mode:

   ```
   crm node standby <node name>
   ```

3. Finally, put the master node into standby mode:

   ```
   crm node standby <node name>
   ```

Installing the MAM Connector Software

Complete the following process on the cluster master and slave nodes.

To install the MAM Connector:

1. If you have not already done so, navigate to the directory containing the installation script:

   ```
   cd /<path>
   ```

2. Run the MAM Connector installation script:

   ```
   ./install.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   The process should complete with information similar to the following:

   ```
   Installed:
     avid-interplay-central-mam.noarch <version>.<build>
     avid-mcux-process-dashboard-pane.noarch <version>.<build>
   
   Complete!
   ```

3. Further verify the success of the installation using the Linux rpm command:

   ```
   rpm -qa | grep mam
   ```

   The output should include the following line:

   ```
   avid-interplay-central-mam-<version>.<build>.noarch.rpm
   avid-mcux-process-dashboard-pane.noarch <version>.<build>.noarch.rpm
   ```

Bringing the Cluster Back Online

With the installation of the MAM Connector complete on both the Master and Slave nodes, bring the cluster back online.

To bring the cluster online:

1. First, bring the master node back online:

   ```
   crm node online <node name>
   ```

2. Next, bring the slave node online:

   ```
   crm node online <node name>
   ```

3. Finally, bring any load-balancing nodes online:

   ```
   crm node online <node name>
   ```

Checking on the Cluster Status

With the MAM Connector installed, verify that all cluster resources are running and that the Cluster Resource Monitor is free of errors.

To verify the cluster status:

1. Use the Cluster Resource Monitor to verify the status of the cluster:

   ```
   crm_mon -f
   ```

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Review the fail-counts for the cluster resources.

2. If there are fail-counts listed, run the Cluster Resource Manager cleanup command to reset them:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   `<rsc>` is the resource name of interest: AvidIPC, pgsqlDB (or another)

   `<node>` (optional) is the node of interest

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the "everywhere" form of the resource.

   For example, to reset the fail-count for AvidAll resource, issue the following command:

   ```
   crm resource cleanup AvidAllEverywhere
   ```

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

3. Proceed to "Configuring the MAM Connector" on page 215 to update the MediaCentral UX System Settings.

Configuring the MAM Connector

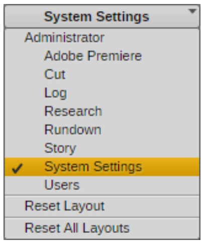
Once the MAM Connector has been installed, the MediaCentral UX System Settings must be configured to connect to Interplay MAM.

To configure the Interplay MAM System Settings:

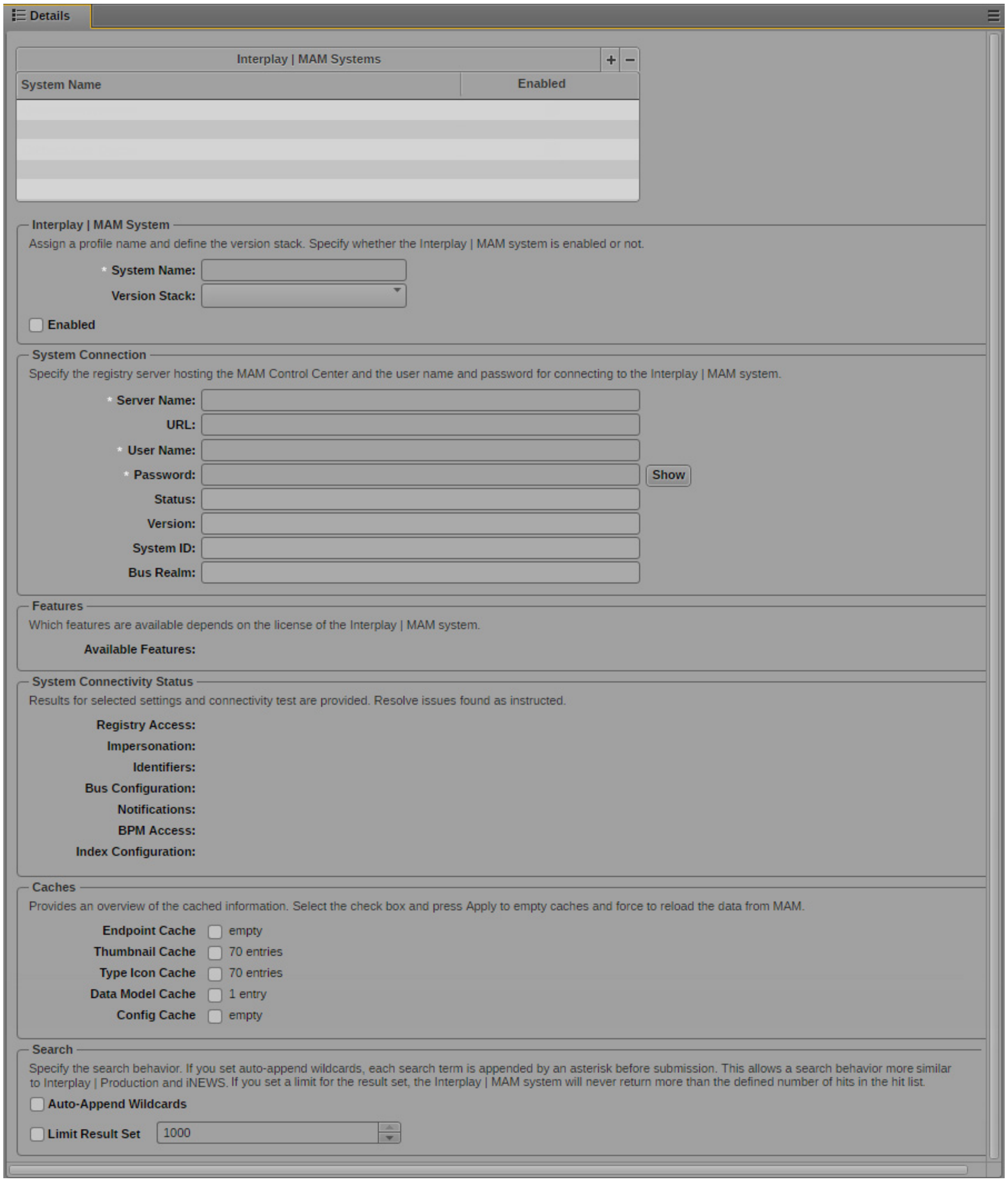
1. Sign into MediaCentral UX as a user with administrator-level access.

   For details on this process, see "Signing into MediaCentral UX" on page 92.

2. Select System Settings from the Layout selector in the upper-right corner of the interface.



3. In the Settings pane, select Interplay | MAM.



Interplay | MAM System

Assign a profile name and define the version stack. Specify whether the Interplay | MAM system is enabled or not.

* System Name:

Version Stack:

□ Enabled

System Connection

Specify the registry server hosting the MAM Control Center and the user name and password for connecting to the Interplay | MAM system.

* Server Name:

URL:

* User Name:

* Password: Show

Status:

Version:

System ID:

Bus Realm:

Features

Which features are available depends on the license of the Interplay | MAM system.

Available Features:

System Connectivity Status

Results for selected settings and connectivity test are provided. Resolve issues found as instructed.

Registry Access:

Impersonation:

Identifiers:

Bus Configuration:

Notifications:

BPM Access:

Index Configuration:

Caches

Provides an overview of the cached information. Select the check box and press Apply to empty caches and force to reload the data from MAM.

Endpoint Cache	□	empty
Thumbnail Cache	□	70 entries
Type Icon Cache	□	70 entries
Data Model Cache	□	1 entry
Config Cache	□	empty

Search

Specify the search behavior. If you set auto-append wildcards, each search term is appended by an asterisk before submission. This allows a search behavior more similar to Interplay | Production and iNEWS. If you set a limit for the result set, the Interplay | MAM system will never return more than the defined number of hits in the hit list.

□ Auto-Append Wildcards

□ Limit Result Set 1000

4. Configure the settings to connect to your Interplay MAM system. For detailed information on the configuration of these settings, see the *Avid MediaCentral | UX Administration Guide*.

Upgrading the MAM Connector

The MAM Connector is upgraded in one of two ways, depending on the version of software you are upgrading from. Reference one of the following sections to upgrade the MAM Connector:

- Upgrading from MAM Connector v2.6 or Higher
- Upgrading from MAM Connector v2.5 or Earlier

Prior to upgrading, note the following:

The MAM Connector installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and sign off during the upgrade procedure.

After upgrading to MCS v2.7 or later, you need to add the IP addresses of the MAM servers to the avd-acs-gateway configuration file. For more information, see "Configuring Access for External Systems" on page 78. If you are connecting to Interplay MAM v5.6, you must configure the ACS gateway port in MAM. For more information, see "Configuring Interplay | MAM for Use with MediaCentral | UX" in the MAM Installation Manual v5.6 or later.

⚠ **Starting with Interplay MAM Connector v2.6.0, the system connection settings are changed and use the MAM Control Center to deliver the credentials of the impersonating user login and registry endpoint URL.**

Upgrading from MAM Connector v2.6 or Higher

The process for upgrading an existing installation of the MAM Connector involves a few simple steps:

To upgrade the MAM Connector:

1. You must first uninstall the existing version of the software.

   For more information, see "Uninstalling the MAM Connector" on page 219.

2. Once the previous version is removed, install the updated version of the MAM Connector. Refer to one of the following sections:

   - "Installing the MAM Connector on a Single Server" on page 212
   - "Installing the MAM Connector in a Cluster" on page 213

3. Clear the Google Chrome (Windows) or Safari (Mac OS) browser cache.

Upgrading from MAM Connector v2.5 or Earlier

MAM Connector v2.6 introduced changes that require the user to complete additional steps to upgrade the software. Refer to the following process to upgrade the MAM Connector, making sure to complete the steps in the order represented below:

1. Clean the previously configured Interplay MAM systems from the ACS Bus.

   For more information, see "Cleaning Up Interplay | MAM Systems" on page 218.

2. Uninstall the existing version of the MAM Connector.

   For more information, see "Uninstalling the MAM Connector" on page 219.

3. Install the updated version of the MAM Connector.

   For more information, see “Installing the MAM Connector on a Single Server” on page 212 or “Installing the MAM Connector in a Cluster” on page 213.

4. Clear the Google Chrome (Windows) or Safari (Mac OS) browser cache.

5. Register and configure the Interplay MAM systems through MediaCentral UX.

   For more information, see “Configuring Interplay | MAM System Settings” on page 218.

Cleaning Up Interplay | MAM Systems

If you are upgrading from MAM Connector v2.5.x or earlier, you need to clean up the previously configured Interplay MAM systems from the ACS Bus Attribute Service.

The following procedure removes all information about connected Interplay MAM systems and their settings from the ACS Bus. Before completing this process, make note of the connection details through the MediaCentral UX System Settings. This information must be manually reentered once the upgrade is complete.

To clean up previously configured Interplay MAM systems:

1. Log into the MCS server as the root user. If you are in a cluster configuration, connect to the cluster master node.

2. Stop the avid-interplay-central service.

   - For a single-server system, enter the following command:

     ```
     service avid-interplay-central stop
     ```

   - In a cluster configuration, all nodes must be taken offline to stop the Pacemaker resource that manages the avid-interplay-central service.

     For details, see “Taking the Cluster Offline” on page 214.

3. Delete the current Interplay MAM systems:

   ```
   acs-query --serviceType=avid.acs.attributes --op=delete --
   paramSet='{"selector":{"name":"InterplayMAM"}}' --serviceVersion=0
   ```

4. Proceed to “Uninstalling the MAM Connector” on page 219 to continue the upgrade of the MAM Connector.

Configuring Interplay | MAM System Settings

Once the upgrade from MAM Connector v2.5 or earlier is complete, you need to register and configure the Interplay MAM systems again using MediaCentral UX.

If you are upgrading from MAM Connector v2.6 or later, this process is not required.

Starting with MAM Connector v2.6, you must provide the MAM Control Center credentials. See step 4 in the following procedure.

To configure Interplay MAM settings:

1. Sign in to MediaCentral UX as an administrator.

2. Select System Settings from the Layouts list.

3. Click the Settings pane menu button and select Add Interplay | MAM.

4. Configure at least the mandatory Interplay MAM system settings:
   a. Specify the Interplay MAM system name.
   b. Enter the host name or IP address of the server where the MAM Control Center is running in the Server Name field.

      Alternatively, change the server name of the automatically generated MAM Control Center base URL https://<*servername*>:9911/ControlCenter in the URL field.
   c. Enter the user name to sign-in to MAM Control Center. The user must be a member of the "MAM Administrators" group for MAM Control Center. This means you must have a Windows account on Interplay MAM side that is in your Windows "MAM Administrators" group that can be used by MediaCentral for the MAM connection.
   d. Enter the password to sign-in to MAM Control Center.

   For complete configuration instructions, see the *Avid MediaCentral UX Administration Guide*.
5. Click Apply.
6. Repeat steps 3 through 5 for all Interplay MAM systems that need to be reconnected.
7. Sign out from MediaCentral UX.

Uninstalling the MAM Connector

In the event that you need to disable the functionality added by the MAM Connector, use one of the following processes to uninstall the software.

This process will disconnect any users currently working on the system. Make sure all users save their work prior to completing this process.

Uninstalling the MAM Connector on a Single Server

To uninstall the software on a single server:

1. Navigate to the directory containing the MAM Connector installation files:

   ```
   cd /<path>
   ```
2. Run the MAM Connector uninstall script:

   ```
   ./uninstall.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   The software is uninstalled.
3. If you are running a single server configuration, restart the avid-interplay-central service:

   ```
   service avid-interplay-central restart
   ```

   This step is not required on a cluster since the process for taking the cluster offline stops the cluster resources and associated services.

Uninstalling the MAM Connector on a Cluster

To uninstall the MAM Connector on a cluster:

1. Verify the current Master, Slave, and load balancing nodes.

   For more information, see "Identifying the Master, Slave, and Load-Balancing Nodes" on page 213.

2. Take all nodes offline.

   For more information, see "Taking the Cluster Offline" on page 214.

3. Starting with the master node, navigate to the directory containing the MAM Connector installation files:

   ```
   cd /<path>
   ```

4. Run the MAM Connector uninstall script:

   ```
   ./uninstall.sh
   ```

   The period-slash "./" in this command tells Linux to look for the script in the current directory.

   If you are in a cluster configuration, complete this step on the master and slave nodes.

5. Bring the nodes back online.

   For more information, see "Bringing the Cluster Back Online" on page 214.

6. Use the Cluster Resource Monitor to verify the status of the cluster:

   ```
   crm_mon -f
   ```

   - Verify the master, slave, and load-balancing nodes (if applicable) are online.
   - Verify that the AvidIPC resource is online on the master node.
   - Review the fail-counts for the cluster resources.

7. If there are fail-counts listed, run the Cluster Resource Manager cleanup command to reset them:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   <rsc> is the resource name of interest: AvidIPC, pgsqlDB (or another)

   <node> (optional) is the node of interest

If you receive an "object/attribute does not exist" error message, it indicates the resource is active on more than one node. Repeat the command using the "everywhere" form of the resource.

For example, to reset the fail-count for AvidAll resource, issue the following command:

```
crm resource cleanup AvidAllEverywhere
```

You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.

13 Multi-Zone

Chapter Overview

The purpose of this chapter is to provide instructions on setting up a multi-zone environment. Configuration of a multi-zone workflow can be completed during the initial system installation or added to systems in an established environment. The procedures in this section must be completed on single server or clustered systems that are fully configured.

The following table describes the topics covered in this chapter:

Step	Task	Time Est.
1	Multi-Zone Overview	2 min
	Provides an introduction to the Multi-Zone concept.	
- -	Enabling RabbitMQ Data Encryption Across Zones	*varies*
	If desired, RabbitMQ data can be encrypted to increase security within the network. This is an optional configuration step.	
2	Verifying the RSA Key Folder	10 min
	RSA keys are “digital signatures” allowing one system to access another without requesting credentials. In a new installation, the folder that contains this key will generally not yet exist.	
3	Creating and Installing the RSA Keys	20 min
	The multi-zone services must have access to remote servers directly, without the need to log in. Installing RSA keys creates a network of trust within the zone.	
4	Verifying Access to the Slave Zone	20 min
	Tests the connection to the Slave Zone through an SSH connection.	
5	Creating the Master Zone and Initiating Multi-Zone	10 min
	Once the MCS nodes in the master zone and slave zone(s) are up and running, the multi-zone environment can be initialized.	
6	Adding Slave Zone(s) to the Multi-Zone Environment	5 min
	With the master zone established, slave zone(s) can be added to the configuration.	
7	Validating Multi-Zone Functionality	5 min
	Creating a user with a different role in each zone verifies that the multi-zone environment is working as expected.	
- -	Dismantling a Multi-Zone Environment	5 min
	Instructions for de-registering the multi-zone environment.	

Step	Task	Time Est.
- -	Making Changes to a Multi-Zone Configuration	1 min
	A note regarding making changes to an established Multi-Zone setup.	
- -	Troubleshooting the Multi-Zone Setup	*varies*
	This section offers possible solutions to Multi-Zone setup issues.	

Multi-Zone Overview

By default, each MediaCentral system operates independently, within a single “zone”, where each zone consists of the following:

- One MediaCentral Platform Services single-server or cluster
- One Interplay Production, iNEWS, and / or Interplay MAM database

A multi-zone environment combines two or more single-zone systems together to enable enhanced WAN workflows. The benefits of a multi-zone environment include:

- Multi-zone user management: Centralized user management across all zones.

  In a multi-zone environment, one zone maintains a master copy of the user database. The master zone has the ability to read and write to database while all slave zones have read-only access. All log-in activity in the slave zones is channeled through the master zone. In the event of a network disruption, the slave zones continues to operate in read-only mode until connectivity to the master zone is re-established.

- Multi-zone central index search: Search across multiple databases in different zones.

  If Media Index is configured across the multi-zone environment, users can quickly search for assets across all zones and instantly play the material in the remote zone.

- Multi-zone media asset delivery: Transfer the high-resolution material you found on a remote zone through an indexed search to your local zone.

  If users wish to combine remote assets in local sequences, a transfer of the material from the remote zone to the local zone can be initiated.

The multi-zone configuration process consists of the following steps:

- (Optional) Enabling RabbitMQ Data Encryption Across Zones
- Verifying the RSA Key Folder
- Creating and Installing the RSA Keys
- Verifying Access to the Slave Zone
- Creating the Master Zone and Initiating Multi-Zone
- Adding Slave Zone(s) to the Multi-Zone Environment
- Validating Multi-Zone Functionality

Additional topics related to multi-zone configuration such as dismantling a multi-zone environment and troubleshooting multi-zone are also covered in this chapter.

Some versions of MediaCentral Platform Services are supported in a mixed multi-zone environment, where not all zones are running the same software version. Consult the *MediaCentral Platform Services ReadMe* or the *MediaCentral Platform Services Upgrade Guide* for specific version compatibility information.

Enabling RabbitMQ Data Encryption Across Zones

During the configuration of the multi-zone environment, links are created within RabbitMQ for each zone. These links begin with a "amqp://" prefix. If desired, RabbitMQ communication can be encrypted between zones for enhanced security when transmitting data over public networks. By altering one of the multi-zone configuration files, secure multi-zone links are created in RabbitMQ with a prefix of "amqps://".

Prior to beginning this process, determine which servers will be included in the multi-zone configuration and which zone will be the master zone. This information is required to complete this process.

⚠ **Enabling encryption must be completed prior to configuring multi-zone or Media Index on your MediaCentral servers. Reconfiguring an existing multi-zone system for encryption requires the system administrator to reset Media Index (if applicable) and dismantle the multi-zone configuration. During the Media Index reset procedure, all indexed data is deleted. Recreating the multi-zone and Media Index configuration can be a time consuming process and should be avoided if possible.**

To configure data encryption:

1. Verify that network port 5671 is open between all zones. This might require changes to the house network firewall device.

   For additional information on required multi-zone ports, see the Avid Networking Port Usage Guide on the Avid Knowledge Base.

2. On the master node of the master zone, use the vi editor to alter the avid-acs-federation configuration file:

   ```
   vi /etc/sysconfig/avid-acs-federation
   ```

3. Add the following environment variable to the configuration file:

   ```
   AVID_FEDERATION_SECURITY_ENCRYPTED
   ```

   This information can be added to any new line within the file.

4. Save and exit the vi session. Press <ESC> and type: **:wq**

5. If the master zone is in a cluster configuration, repeat steps 1-4 on the slave node.

6. Repeat steps 1-4 on the remote zones. This includes any zones consisting of a single-server or the master/slave pair of any zone in a cluster configuration.

Editing the configuration file on cluster load-balancing nodes is not required.

Verifying the RSA Key Folder

The multi-zone services must be allowed access to remote MCS servers directly, without the need to provide log-in information. This is accomplished through the use of an RSA key or "digital signature".

Once created, the RSA key is located at: `/root/.ssh/`. Assuming that this is a new installation, this folder will not exist. The following process verifies the existence or contents of this folder.

To verify the RSA folder:

1. Log into each server that will be part of the multi-zone configuration as the root user.
2. List the contents of the `/root/.ssh/` directory:

   ```
   ls /root/.ssh
   ```

   The system should reply with the following:

   ```
   ls: cannot access /root/.ssh/: No such file or directory
   ```

If you are adding multi-zone to an existing MCS installation, your results may vary.

Creating and Installing the RSA Keys

The RSA keys are created on the Master and Slave nodes (if applicable) in the Master Zone and are distributed to all Master and Slave nodes (if applicable) in the Slave Zone(s) in the multi-zone configuration. You do not need to copy the RSA keys to the Load Balancing nodes in any zone.

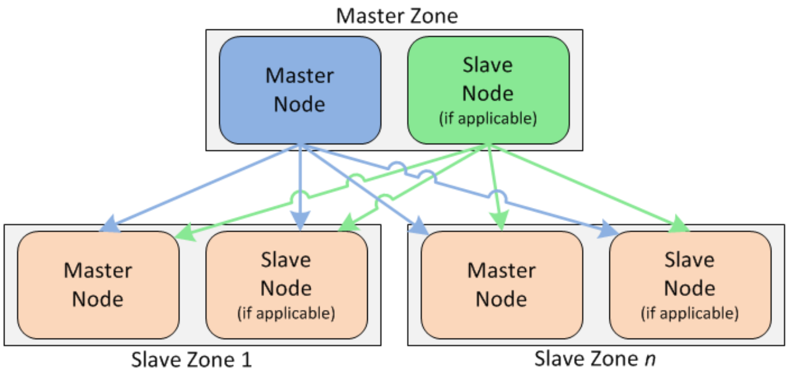
Generate the RSA keys in the Master Zone on the following nodes:

- Master node
- (if applicable) Slave node

Install the generated RSA keys in the slave zone on the following nodes:

- All Master and Slave nodes in the slave zone(s)

The following illustration shows the RSA keys copied from the Master and Slave nodes of the Master Zone to Slave Zone 1 through Slave Zone *n*.


Master Zone
Master Node
Slave Node (if applicable)
Master Node
Slave Node (if applicable)
Slave Zone 1
Master Node
Slave Node (if applicable)
Slave Zone *n*

To generate and install the RSA keys:

1. Log in (at the Linux prompt) to the Master Node in the Master Zone as the root user.
2. Generate the public/private RSA key pair using the RHEL ssh-keygen utility.
   a. Enter the following command to initiate the key generation:

      ```
      ssh-keygen
      ```

   b. Press Enter to accept the default file and location.
   c. Press Enter twice to create and verify a blank passphrase.

The system responds by outputting information similar to the following:

```
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
55:66:25:00:f7:15:d5:cd:30:89:6f:0d:e2:c3:d4:4f root@wavd-
mcs01.wavd.com

The key's randomart image is:
+---[ RSA 2048]---+
|        o.B=+++Bo|
|   .   o = .o.+.E|
|        o  +   + |
|  .    .    +   .|
|        S    .   |
|   o       .     |
| o    o          |
+-----------------+
```

3. Use the RHEL ssh-copy-id utility to add the public key to the list of authorized keys on the Master Node in the Slave Zone:

   ssh-copy-id root@<*hostname*>

   Where <*hostname*> is the short hostname of the Master Node in the Slave Zone.

   The system responds with message similar to the following:

   ```
   The authenticity of host '<hostname> (XXX.XX.XX.XXX)' can't be established.
   Are you sure you want to continue connecting (yes/no)?
   ```

4. Type **yes** to connect to the MCS server.

   The system responds with message similar to the following:

   ```
   Warning: Permanently added '<hostname>, XXX.XX.XX.XXX' (RSA) to the list of
   known hosts.

   root@<hostname>'s password:
   ```

5. Enter the password for the root user of the remote system.

   The system responds with message similar to the following:

   ```
   Now try logging into the machine, with "ssh 'root@<hostname>'", and check
   in:
     .ssh/authorized_keys
   to make sure we haven't added extra keys that you weren't expecting.
   ```

   With the RSA key in place, multi-zone processes can now gain access to the remote server automatically (without the need to provide root user credentials).

6. (if applicable) Repeat steps 3 – 5 to copy the RSA key to the Slave Node of the Slave Zone.

7. (if applicable) If your Slave Zone is a cluster, repeat steps 3 – 5 to copy the RSA key to the IP address of the Slave Zone's cluster IP address.

When copying the RSA to the cluster IP address, you will be asked to verify that you wish to connect, but you will not be asked to verify a password.

8. (if applicable) Repeat steps 3 – 7 to copy the RSA key from the Master Node of the Master Zone to the Master and Slave nodes of additional Slave Zones.

9. (if applicable) Repeat steps 1 – 7 to copy the RSA key from the Slave Node of the Master Zone to the Master and Slave nodes of all Slave Zones.

Verifying Access to the Slave Zone

This process tests the connection to the Master and Slave nodes of the Slave Zone(s) by attempting an SSH connection. It also establishes a connection to remote MCS clusters which is very important when adding Slave Zones to the multi-zone configuration.

To verify slave zone access:

1. From the Master Node of the Master Zone, make a connection to one of the servers in the Slave Zone:

   ```
   ssh root@<hostname>
   ```

   Because of the RSA keys created in the previous step, you should be logged into the server without being prompted for a password. Also notice that the Linux prompt now indicates the hostname of the remote server.

2. List the contents of the directory containing the RSA key:

   ```
   ls /root/.ssh/
   ```

   You should see the new RSA key “authorized_keys” listed.

3. Return to your original session by entering the following command:

   ```
   exit
   ```

   The Linux prompt should now indicate the hostname or IP of your original server.

4. Repeat steps 1 – 3 for all Master and Slave nodes in all Slave Zones.

5. From the Slave Node of the Master Zone, repeat steps 1 – 4 to ensure that the Slave Node can make a secure connection to all Master and Slave nodes in all Slave Zones.

6. If your Slave Zone consists of a cluster, make a connection to the cluster’s IP address.

   a. Make a connection to the Slave Zone cluster IP from the Master Node of the Master Zone:

      ```
      ssh root@<cluster IP>
      ```

      Because the RSA keys were not copied to the cluster, you will be prompted for a password. Enter the root user password for the cluster’s Master / Slave node.

   b. Return to your original session with the following command:

      ```
      exit
      ```

   c. If you have additional Slave Zones, repeat these steps for each cluster.

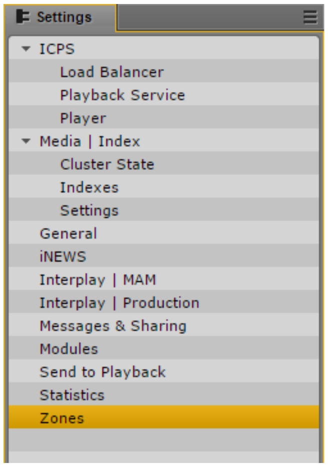
   d. Repeat these steps for each Slave Zone cluster from the Slave Node in the Master Zone.

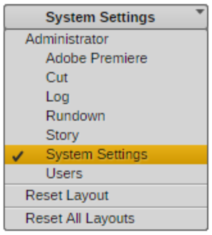
Creating the Master Zone and Initiating Multi-Zone

This process begins the creation of the multi-zone environment by creating the Master Zone.

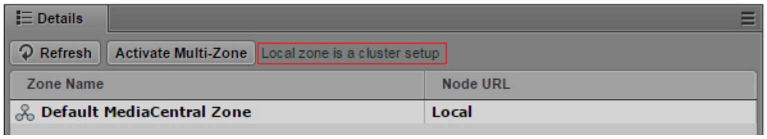
To create the multi-zone master zone:

1. Sign in to the MediaCentral UX master zone as a user with administrator-level access.
2. Select System Settings from the Layout selector.
3. In the Settings pane, click Zones.





The Details pane appears on the right side of the screen. This pane displays the currently active zone(s). For now, only the "default" zone exists.



Local zone is a cluster setup

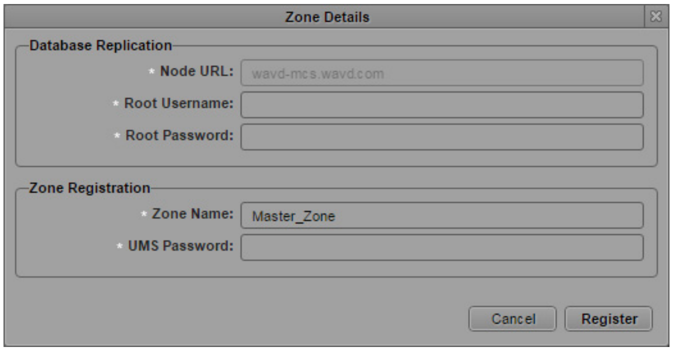
Zone Name	Node URL
Default MediaCentral Zone	Local

Text to the right of the "Activate Multi-Zone" button indicates if the Master Zone is a single machine or cluster configuration.

4. Click the Activate Multi-Zone button to begin the setup process.

   A confirmation dialog box appears prompting you to verify that you wish to continue.

5. Click Proceed and complete the required fields in the Zone Details window:



Database Replication

* Node URL: wavd-mcs.wavd.com
* Root Username:
* Root Password:

Zone Registration

* Zone Name: Master_Zone
* UMS Password:

Database Replication:

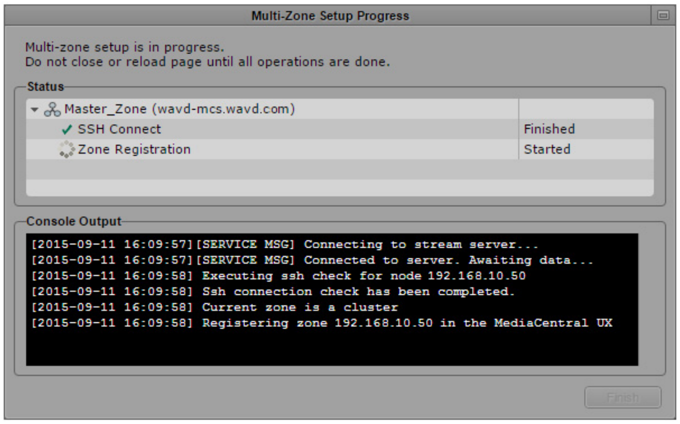
- The Node URL lists the FQDN you entered in the web browser to access MediaCentral UX. This field cannot be altered.
- Root Username and Root Password: The root user credentials for the master zone MCS server.

Zone Registration:

- Zone Name: Name of the master zone (e.g. Master_Zone).
- UMS Password: Enter the MediaCentral UX Administrator password of the master zone.

6. Click Register.

   A dialog appears showing progress of the operations related to zone creation.



Multi-Zone Setup Progress

Multi-zone setup is in progress.
Do not close or reload page until all operations are done.

Status

Master_Zone (wavd-mcs.wavd.com)	
✓ SSH Connect	Finished
Zone Registration	Started

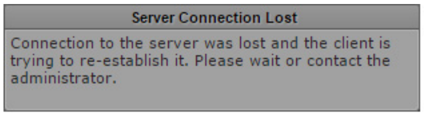
Console Output

```
[2015-09-11 16:09:57][SERVICE MSG] Connecting to stream server...
[2015-09-11 16:09:57][SERVICE MSG] Connected to server. Awaiting data...
[2015-09-11 16:09:58] Executing ssh check for node 192.168.10.50
[2015-09-11 16:09:58] Ssh connection check has been completed.
[2015-09-11 16:09:58] Current zone is a cluster
[2015-09-11 16:09:58] Registering zone 192.168.10.50 in the MediaCentral UX
```

   Once complete, a SUCCESS message will appear within the progress window.

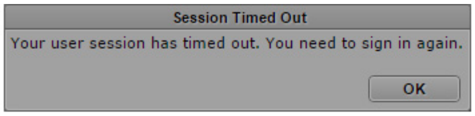
7. Click the Finish button to complete the process.

   Some services are restarted during this period. You may see one or both of the following messages:



Server Connection Lost

Connection to the server was lost and the client is trying to re-establish it. Please wait or contact the administrator.



Session Timed Out

Your user session has timed out. You need to sign in again.

   Click OK in the “Session Timed Out” window.

8. You will be logged out of MediaCentral UX at this time.

Adding Slave Zone(s) to the Multi-Zone Environment

If you are adding a slave zone as part of a new installation, continue with this process. If you are adding a slave zone to an existing installation, review the following steps before continuing:

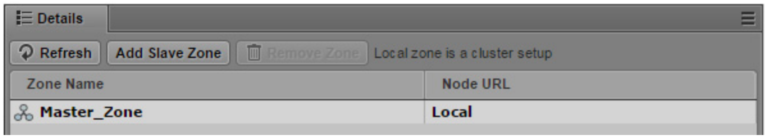
- “Multi-Zone Overview” on page 223
- “Verifying the RSA Key Folder” on page 224
- “Creating and Installing the RSA Keys” on page 225
- “Verifying Access to the Slave Zone” on page 227

To add a slave zone to the configuration:

1. Sign in to the MediaCentral UX master zone as a user with administrator-level access.

2. Select System Settings from the Layout selector and Zones in the Settings pane.

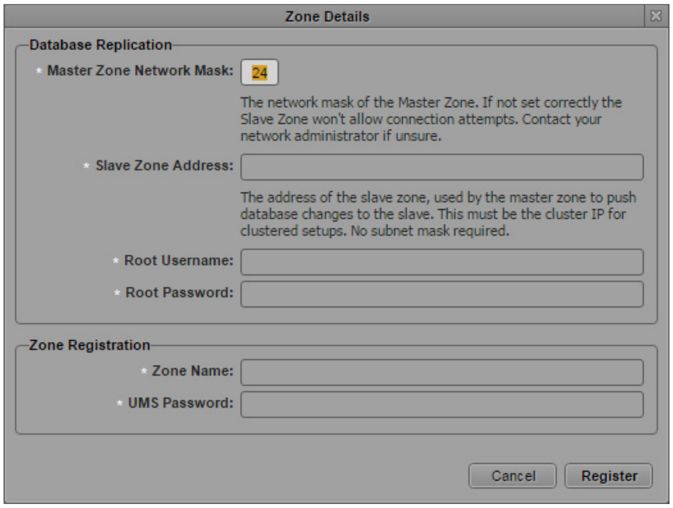
   The Zones Details area shows the information for the master zone (e.g. Master_Zone):



Local zone is a cluster setup

Zone Name	Node URL
Master_Zone	Local

3. Click the Add Slave Zone button. The Zone Details dialog appears:



Zone Details

Database Replication

* Master Zone Network Mask: 24

The network mask of the Master Zone. If not set correctly the Slave Zone won't allow connection attempts. Contact your network administrator if unsure.

* Slave Zone Address:

The address of the slave zone, used by the master zone to push database changes to the slave. This must be the cluster IP for clustered setups. No subnet mask required.

* Root Username:

* Root Password:

Zone Registration

* Zone Name:

* UMS Password:

4. In the Zone Details dialog, enter the following information:

   Database Replication:

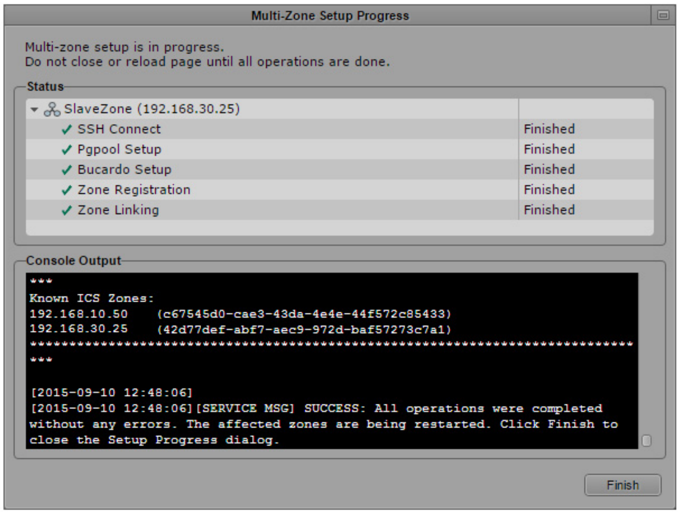
   - Master Zone Network: Specify the IP range for this network (e.g. 23, 24, 25)
   - Slave Zone Address: Specify the IP address of the slave zone. This is either the IP address of a single server or the IP address of a multi-server cluster.
   - Root Username and Root Password: Specify the username (root) and password for the slave zone.

   Zone Registration:

   - Zone Name: Name of the slave zone (e.g. Slave_Zone). This name will appear in the “Zone Name” column in System Settings > Zones.
   - UMS Password: Enter the MediaCentral UX Administrator password of the master zone.

5. Click Register.

   A dialog appears showing progress of the operations related to slave zone registration.



Multi-Zone Setup Progress

Multi-zone setup is in progress.
Do not close or reload page until all operations are done.

Status

SlaveZone (192.168.30.25)	
✓ SSH Connect	Finished
✓ Pgpool Setup	Finished
✓ Bucardo Setup	Finished
✓ Zone Registration	Finished
✓ Zone Linking	Finished

Console Output

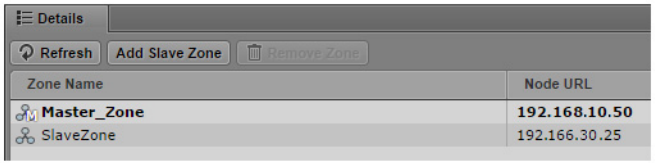
```
***
Known ICS Zones:
192.168.10.50    (c67545d0-cae3-43da-4e4e-44f572c85433)
192.168.30.25    (42d77def-abf7-aec9-972d-baf57273c7a1)
******************************************************************************
***

[2015-09-10 12:48:06]
[2015-09-10 12:48:06][SERVICE MSG] SUCCESS: All operations were completed
without any errors. The affected zones are being restarted. Click Finish to
close the Setup Progress dialog.
```

Once complete, a SUCCESS message appears within the progress window.

6. Click the Finish button to complete the process.

   Any users logged into the slave zone are disconnected as services are restarted on the slave zone.

7. The Zones Details page is refreshed with the new slave zone.



Zone Name	Node URL
Master_Zone	**192.168.10.50**
SlaveZone	192.166.30.25

   Note that the master zone is now identified with the letter “M” and the current zone is shown in bold text. The “current zone” is the zone for the machine where you are currently signed in.

8. Repeat the process to add other slave zones, as desired.

Validating Multi-Zone Functionality

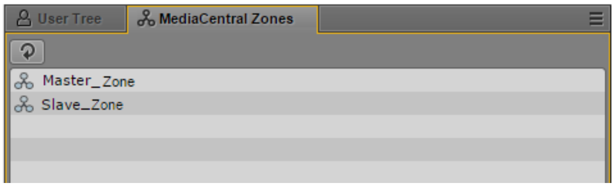
In this step you verify multi-zone UMS functionality by adding creating a user with different roles in each zone.

To validate the multi-zone functionality:

1. Sign in to MediaCentral UX as an administrator-level user in either the master zone or one of the slave zones.

2. Select Users from the Layout selector.

3. Observe that the Users layout now has an additional tab named MediaCentral Zones, where all the linked zones are displayed.



Master_Zone
Slave_Zone

4. To validate that a user added to one zone can sign in from another, begin by clicking the Create User button.

   In the Details pane, type the properties for the new user, at the very least:

   - User name (e.g. multizone_test)
   - Password
   - To simplify the test, uncheck “User must change password at next sign-in”

5. Drag a role for the user from the Roles pane to the Role section of the Details pane for the new user.

   Notice that you can assign the multi-zone user a different role in each zone. For example, the user can be an administrator in one zone, and a media logger in another.

6. Click the Save button to save your changes.

   The new user is added to the User Tree, and the Details pane is populated with the layouts available to the user in each zone.

7. Finally, sign in to MediaCentral UX in the other zone using the newly created multi-zone user.

   Note the following:

   - If you sign in to a slave zone, the user credentials are being validated in the master zone.
   - The available layouts are those you assigned for the user upon creation.

8. Once the master and slave zones have been configured and validated, see "Sharded MongoDB" on page 129 to reconfigure the zones for a sharded Mongo configuration.

Dismantling a Multi-Zone Environment

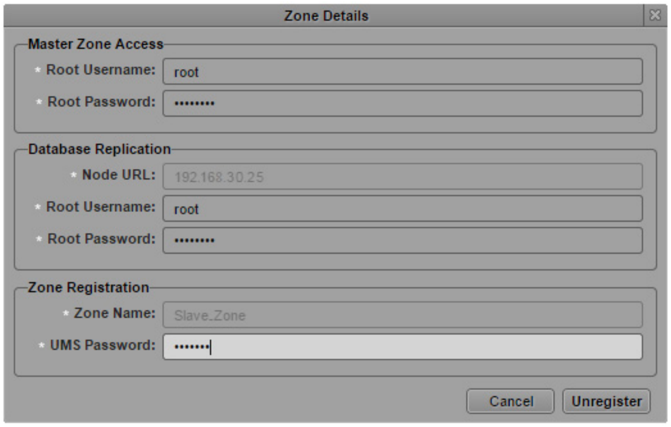
When a multi-zone environment is no longer required, it can be dismantled. Dismantling a multi-zone environment removes all roles for multi-zone users (login credentials remain). If you later use the same user names on independent systems, you need to manually re-assign the roles on each system.

If Media | Index has been configured on the zone you plan to unregister from the multi-zone environment, make sure to remove the zone from the Elasticsearch tribe configuration prior to altering the multi-zone setup. This is required because Media Index depends on some of the inter-service communication features built into multi-zone. For more information on removing an index, see the Avid Media | Index Configuration Guide.

To dismantle the multi-zone:

1. Sign in to MediaCentral UX in the Master Zone as the Administrator user.
2. Select System Settings from the Layout selector and Zones in the Settings pane.
3. For each Slave Zone, select the zone and click the Remove Zone button.

   The Zone Details dialog appears for the slave zone.



Zone Details

Master Zone Access

* Root Username: root
* Root Password: ••••••••

Database Replication

* Node URL: 192.168.30.25
* Root Username: root
* Root Password: ••••••••

Zone Registration

* Zone Name: Slave_Zone
* UMS Password: •••••••

4. In the Zone Details dialog, enter the following information:

   Master Zone Access:

   - Root Username and Root Password: The root user credentials for the Master Zone MCS server.

Database Replication:

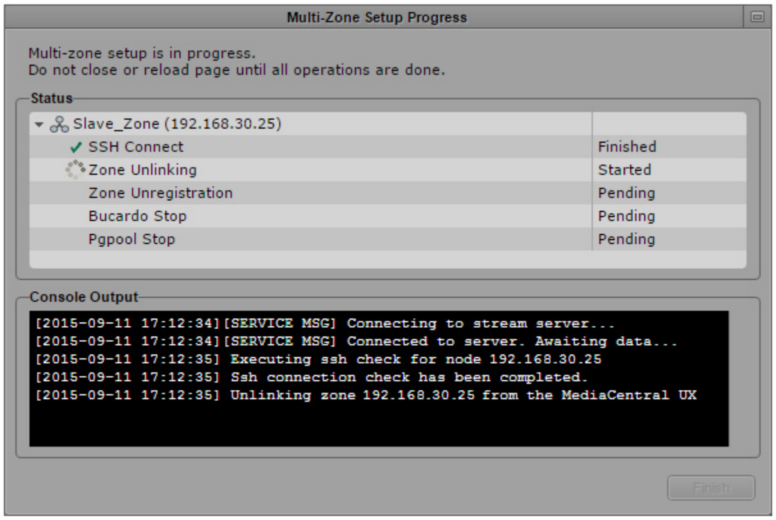
- Node URL: This field is completed for you. This is the IP address of the MediaCentral instance / cluster in the Slave Zone.
- Root Username and Root Password: This is the root user of the Slave Zone.

Zone Registration:

- Zone Name: This field is completed for you. This is the name of the slave zone (e.g. Slave_Zone).
- UMS Password: MediaCentral UX Administrator password for Slave Zone.

5. Click the Unregister button.

   A dialog appears showing progress of the operations related to slave zone deregistration.



Multi-Zone Setup Progress

Multi-zone setup is in progress.
Do not close or reload page until all operations are done.

Status

Slave_Zone (192.168.30.25)	
✓ SSH Connect	Finished
Zone Unlinking	Started
Zone Unregistration	Pending
Bucardo Stop	Pending
Pgpool Stop	Pending

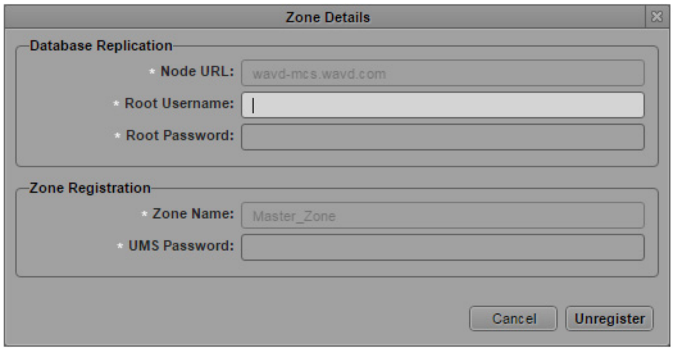
Console Output

```
[2015-09-11 17:12:34][SERVICE MSG] Connecting to stream server...
[2015-09-11 17:12:34][SERVICE MSG] Connected to server. Awaiting data...
[2015-09-11 17:12:35] Executing ssh check for node 192.168.30.25
[2015-09-11 17:12:35] Ssh connection check has been completed.
[2015-09-11 17:12:35] Unlinking zone 192.168.30.25 from the MediaCentral UX
```

   Any users logged into the slave zone are disconnected as services are restarted on the slave zone.

6. Click the Finish button to close the deregistration window.
7. Repeat for any other Slave Zones you wish to remove.
8. Once deregistration of the slave zone is complete, select the Master Zone and click the Remove Zone button.

   The Zone Details dialog appears for the master zone.



Zone Details

Database Replication

* Node URL: wavd-mcs.wavd.com
* Root Username:
* Root Password:

Zone Registration

* Zone Name: Master_Zone
* UMS Password:

9. In the Zone Details dialog, enter the following information:

   Database Replication:

   - Node URL: This field is completed for you. This is the IP address of the MediaCentral instance / cluster in the Master Zone.
   - Root Username and Root Password: This is the root user of the Master Zone.

   Zone Registration:

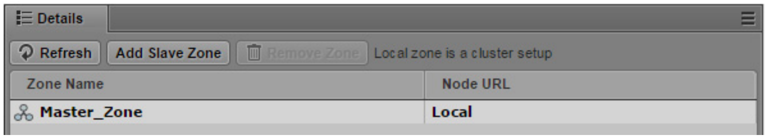
   - Zone Name: This field is completed for you. This is the name of the master zone (e.g. Master_Zone).
   - UMS Password: MediaCentral UX Administrator password for Master Zone.

10. Click the Unregister button

    A dialog appears showing progress of the operations related to master zone deregistration.

    Any users logged into the slave zone are disconnected as services are restarted on the slave zone.

11. Click the Finish button to close the deregistration window.
12. Some services are restarted during this period. You might see one or both of the following messages:



Local zone is a cluster setup

Zone Name	Node URL
Master_Zone	Local

    Click OK in the “Session Timed Out” window.

13. You are logged out of MediaCentral UX at this time.

Making Changes to a Multi-Zone Configuration

If changes are made to the multi-zone configuration after the initial setup, the MCS messenger service must be restarted on all nodes. Examples of such changes include: altering information contained in the initial multi-zone configuration process; adding or removing a zone.

To restart the messenger service, log in to each node of the cluster and type the following command:

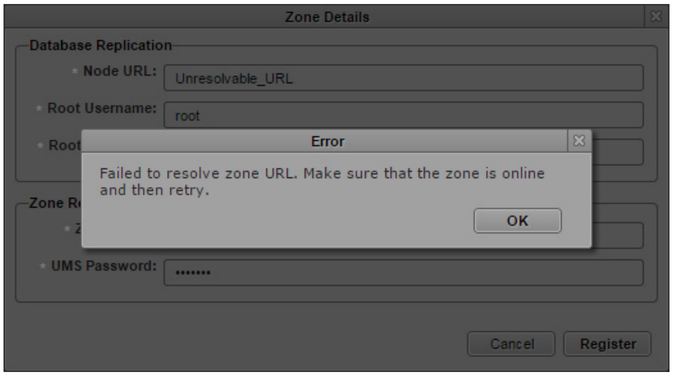
```
service avid-acs-messenger restart
```

Troubleshooting the Multi-Zone Setup

This section contains suggestions for troubleshooting the multi-zone configuration process.

Failed to Resolve Zone URL

When registering the slave zone the following message indicates the zone is unreachable. Verify that the zone is online and the URL you entered is correct.

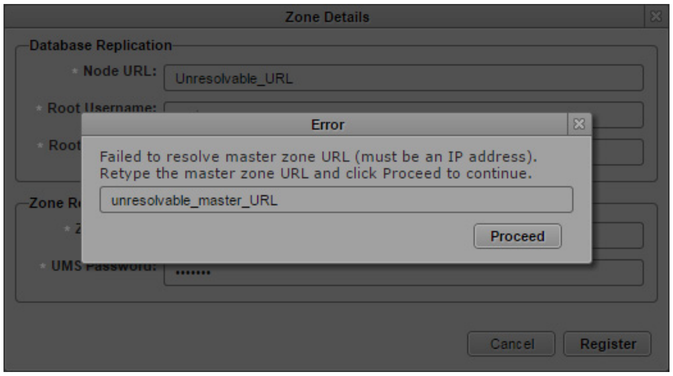


Unresolvable_URL

root

Failed to resolve zone URL. Make sure that the zone is online and then retry.

The master zone URL is passed into the zone configuration processes automatically, based on the current URL as shown in the browser. If you receive the following error, it may indicate the browser is using a form that is unreachable to the backend services (e.g. a hostname). Re-enter the address as an IP address and try again.



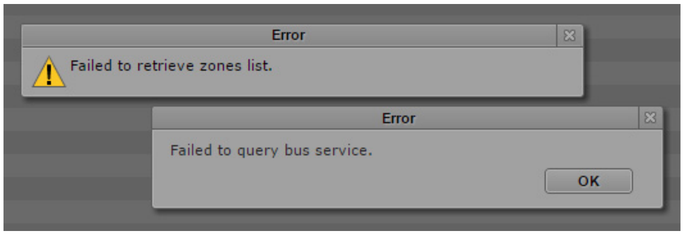
Unresolvable_URL

Failed to resolve master zone URL (must be an IP address). Retype the master zone URL and click Proceed to continue.

unresolvable_master_URL

Bus Error

If a “failed to query bus service” error appears, check that the ACS bus is running in a command shell.

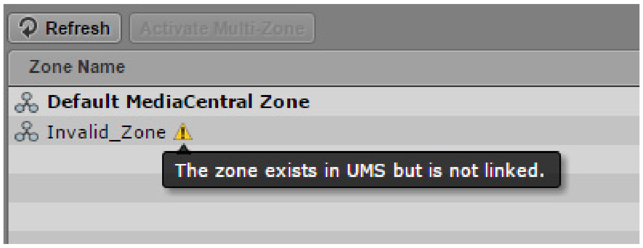


Failed to retrieve zones list.

Failed to query bus service.

Errors in Zone Configuration

An exclamation point next to a zone indicates incorrect configuration.



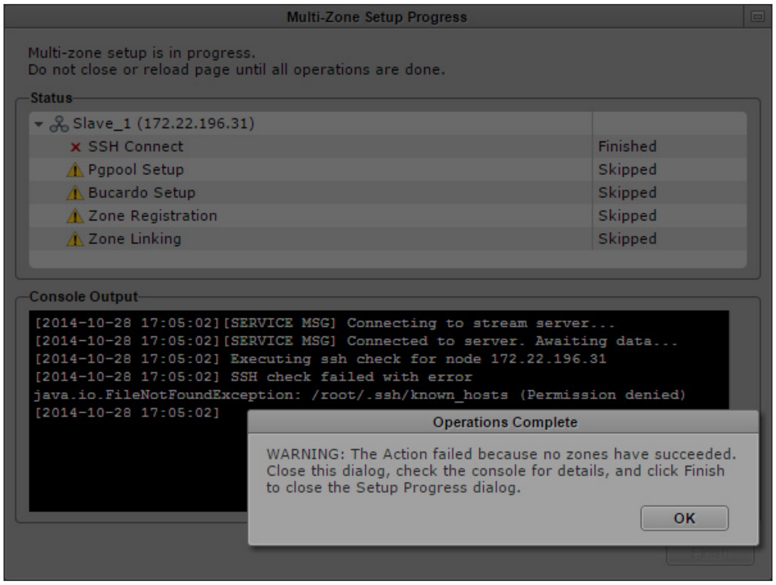
Zone Name
Default MediaCentral Zone
Invalid_Zone ⚠

The zone exists in UMS but is not linked.

Message	Explanation
The zone does not exist in the UMS.	Zone is present in the BUS, but not in the UMS.
The zone exists in UMS but is not linked.	Zone is present in the UMS, but not in the BUS.
Some links are missing.	The zone is missing one or more links to other zones.

Errors During Setup

If any stage of the setup fails, all the subsequent steps are skipped. In this case, the problem most likely cannot be fixed through the UI, and must be resolved at the command-line.


Multi-Zone Setup Progress

Multi-zone setup is in progress.
Do not close or reload page until all operations are done.

Status

Slave_1 (172.22.196.31)	
✗ SSH Connect	Finished
⚠ Pgpool Setup	Skipped
⚠ Bucardo Setup	Skipped
⚠ Zone Registration	Skipped
⚠ Zone Linking	Skipped

Console Output

```
[2014-10-28 17:05:02][SERVICE MSG] Connecting to stream server...
[2014-10-28 17:05:02][SERVICE MSG] Connected to server. Awaiting data...
[2014-10-28 17:05:02] Executing ssh check for node 172.22.196.31
[2014-10-28 17:05:02] SSH check failed with error
java.io.FileNotFoundException: /root/.ssh/known_hosts (Permission denied)
[2014-10-28 17:05:02]
```

Operations Complete

WARNING: The Action failed because no zones have succeeded.
Close this dialog, check the console for details, and click Finish
to close the Setup Progress dialog.

A Additional Topics

Chapter Overview

The purpose of this appendix is to provide additional information and detail on topics included in the main body of the Installation Guide.

The following table describes the topics covered in this appendix:

Topic
Copying Software to the MCS Server
Installing MCS on Non-HP / Dell Hardware
Working with the Dell RAID Controller
Card Placement in MCS Servers
Enabling Trusted Certificates
Port Requirements
Contents of the MCS Installation Package
Determining the Installed MCS Version
Using the MediaCentral Health Check Script
Enabling the Player Demonstration Web Page
Verifying Cache Directory Permissions
Modifying application.properties
Working with the MediaCentral UX Configurator
Backing up and Restoring the MCS Database
Working with the Avid Shared Storage Client
Additional information on Clustering

Copying Software to the MCS Server

At various times during the installation, you are required to copy software to the MCS server. The following two processes are provided as examples of how to complete this task:

- Using an SFTP application on an external system
- Connecting a USB drive directly to the server

While the SFTP method may be preferred for ease of access, the USB method might be required for some operations such as backing up MCS files during a system upgrade.

Copying Software Using an SFTP Client

Files can be copied to and from the Linux server through the use of a secure shell (SSH) file transfer protocol (FTP) client — commonly abbreviated SFTP. WinSCP (Windows) and muCommander (Mac) are free, open-source clients that can securely copy files between Linux and Windows or Mac operating systems. FileZilla, another free open-source utility, can be used in the same way and has the advantage of being available for both Windows and Mac.

The process below uses WinSCP as an example of an SFTP client.

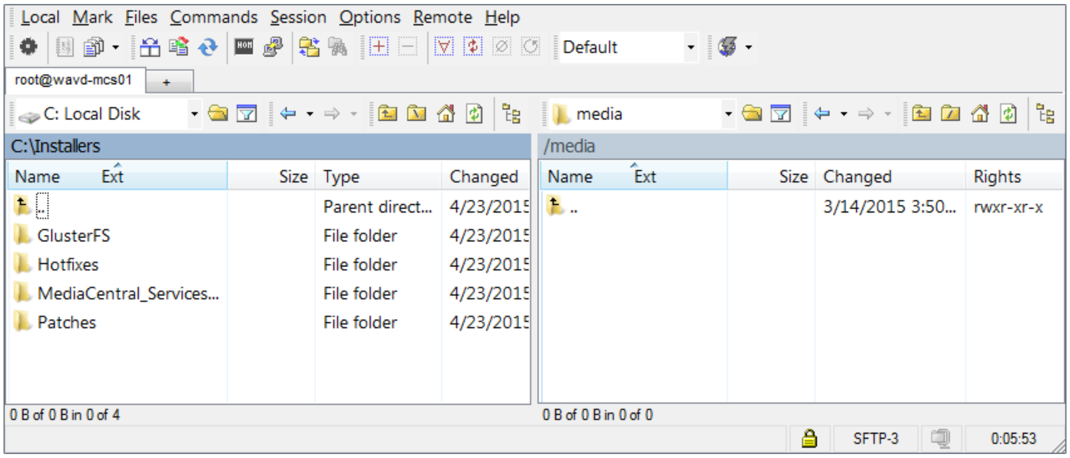
To copy software using an SFTP client:

1. Download and install the WinSCP software on a Windows system that has network access to the MCS server.

   WinSCP can be downloaded from the following location: http://winscp.net
2. Launch WinSCP.
3. Click the New button and enter the Host name (or IP address) of your server, User name (root), and Password.
4. Click Login.

   The following warning message is displayed: “Continue connecting and add host key to the cache?”
5. Click Yes.

   The WinSCP interface is displayed. The left pane represents your source Windows system. The right pane represents your MCS server.



C:\Installers

Name	Ext	Size	Type	Changed
..			Parent direct...	4/23/2015
GlusterFS			File folder	4/23/2015
Hotfixes			File folder	4/23/2015
MediaCentral_Services...			File folder	4/23/2015
Patches			File folder	4/23/2015

0 B of 0 B in 0 of 4

/media

Name	Ext	Size	Changed	Rights
..			3/14/2015 3:50...	rwxr-xr-x

0 B of 0 B in 0 of 0

SFTP-3 0:05:53

6. Navigate to the location of the downloaded MCS installation files in the left pane.
7. Navigate to the `/media` folder on the MCS server in the right pane.
8. Create a directory structure for the MCS installer:

   a. Right-click in the right pane and select New > Directory.

   b. In the “New folder name” field, type **`installers`** and click OK.

   c. Double-click on the new `installers` folder in the right pane.

   d. When copying the MCS installer to the server, the installer must be contained in its own folder. Create a sub folder for the MCS installer:

   Example: `/media/installers/MCS_2.9.0`

When manually creating folders, avoid spaces and other illegal Linux characters. Installations will fail if spaces or illegal characters are encountered in the file path.

   e. Drag and drop the files or folders you wish to copy from the left pane to the right.

   Depending on your WinSCP settings, you might see a dialog box asking if you want to copy the files to the remote directory. If asked, click Copy.

9. After all desired files or folders have been copied, close WinSCP.

Copying Software Using a USB Drive

For simply mounting and unmounting a USB drive, follow the process below and eliminate steps 7, 8, and 9.

To copy software using a USB drive:

1. Insert the USB drive into the MCS server.
2. Use the display message command to verify the name of the device:

   ```
   dmesg
   ```

   Information relating to the hardware appears on the screen.

   Information for the USB drive will appear near the end of the output, near the list of SCSI devices. The name of the USB drive is found inside square brackets (for example, sdc). This is the name you use to mount the drive.

   The dmesg command displays a great deal of information which can be difficult to review, given the limited size of the VM display window. You can reduce the amount of information that dmesg returns by using the Linux `grep` command to show only items that contain certain text (such as “sd”) and the `more` command to display only one page of information at a time. The following command can be used as an alternative:

   ```
   dmesg | grep sd | more
   ```

   Press the space bar to display additional pages.

3. If needed, create a mount point for the USB drive:

   ```
   mkdir /media/usb
   ```

4. Mount the USB drive at the mount point you just created:

   ```
   mount /dev/sdc1 /media/usb
   ```

Note the name of the USB drive, sdc (in this case) takes a 1 (one) in the mount command. This simply indicates a partition exists on the drive. When the USB drive was formatted, the partition was created.

The USB drive is now mounted and available for use.

5. Verify the USB drive has been mounted:

   ```
   df -h
   ```

   Information is displayed about all mounted file systems and devices, and should include information about the USB drive, similar to the following (some output omitted for clarity):

   ```
   Filesystem        Size Used Avail Use% Mounted on

   /dev/sdc1         7.5G 5.3G  2.2G  71% /media/usb
   ```

6. To change to the mount point:

   ```
   cd /media/usb
   ```

7. If necessary, create a directory for the installer packages:

   ```
   mkdir /media/installers
   ```

8. When copying the MCS installer to the server, the installer must be contained in its own folder. Create a sub folder for the MCS installer:

   ```
   mkdir /media/installers/MCS_2.9.0
   ```

When manually creating folders, avoid spaces and other illegal Linux characters. Installations will fail if spaces or illegal characters are encountered in the file path.

9. Copy files to the MCS server:

   - For a single file:

     ```
     cp filename /media/installers/MCS_2.9.0
     ```

   - For a folder:

     ```
     cp -R foldername /media/installers/MCS_2.9.0
     ```

10. Once you have finished copying all necessary files, you must navigate away from the current directory. RHEL will not unmount the USB drive if it is the current active directory. Type the following to navigate to the `/root` home directory:

    ```
    cd
    ```

11. Unmount the USB drive from the server:

    ```
    umount /media/usb
    ```

    If you receive an error message that the USB device is busy, it typically indicates the Linux ISO on the USB drive was auto-mounted. Verify what is mounted using the `df -h` command, the `mount` command, or both. Then dismount the Linux ISO first, followed by the USB device:

    ```
    umount /sysinstall
    ```

    ```
    umount /media/usb
    ```

12. Remove the USB drive from the server.

Once you have copied the necessary software, make sure you unmount and remove the USB drive from the server. If you re-boot with the server with the USB drive still in place, RHEL will be re-installed and all your work will be lost.

Installing MCS on Non-HP / Dell Hardware

MCS supports MediaCentral UX and MediaCentral Cloud on specific HP and Dell servers. Therefore, this section does not pertain to those deployments. Installing MCS on non-HP or Dell hardware is only supported for Interplay MAM deployments

For more information on MCS qualified hardware, see the *MediaCentral Platform Services Hardware Guide* on the Avid Knowledge Base.

The primary difference between installing MCS on known platforms (HP or Dell) and "unknown" platforms is the use of a RHEL "kickstart" file. A kickstart file (ks.cfg) is a Linux convenience that accelerates the installation process by automatically answering some questions for "known hardware".

The kickstart assisted installation process of RHEL and MCS should not be followed for configurations the do not include HP or Dell hardware. RHEL and MCS must be installed separately because there is no guarantee that the supplied kickstart file will work on other hardware. However, you can examine the contents of the kickstart file and mimic its behavior during a manual installation, or create a kickstart file for your custom hardware. As previously stated, the kickstart file is a convenience and the creation of a kickstart file is not required.

MediaCentral Platform Services requires three partitions on the (mirrored) system drive:

- The first is the boot partition (/boot).
- The second is the DRBD (Distributed Replicated Block Device) storage system partition. In a clustered configuration, MCS uses DRBD to replicate its PostgreSQL database.
- The third is the system partition (/).

On HP and Dell hardware, the kickstart file on the MCS Installation USB Drive creates the partitions on the system drive automatically. On other servers these partitions must be created manually.

The DRBD partition on the system drive is required only for cluster deployments. However, Avid best practices suggest that you created all three system partitions to enable future system expansions to a clustered configuration.

This process requires a RHEL DVD or RHEL.iso file. Log in to your Red Hat Network account and download the DVD image (.iso) file or purchase a physical DVD. Either format can be used for the MCS installation. At the time of this document's publication, the RHEL v6.5 ISO could be found on the RHEL website by completing the following:

1. Select **Red Hat Enterprise Linux Server** from the Red Hat Product Downloads page.
2. Specify **Red Hat Enterprise Linux Server** (product variant), **6.5** (version) and **x86_64** (architecture)
3. Download the Binary DVD (rhel-server-6.5-x86_64-dvd.iso).

If you are unfamiliar with the manual installation of RHEL, the *MediaCentral Platform Services Virtual Environment with VMware® Best Practices Guide* includes a detailed description of this process and can be used as reference material.

Non-HP / Dell Installation Process

The following presents a high-level overview for completing a manual installation of the Red Hat Enterprise Linux and MediaCentral Platform Services software packages. For a more detailed version of this process, see “Installing RHEL and MediaCentral” the *MediaCentral Platform Services Virtual Environment with VMware Best Practices Guide* on the Avid Knowledge Base.

To install RHEL and MCS on non HP or Dell servers:

1. Configure the server hardware:

   a. Create a RAID 1 (mirror) for the system disk using the hardware BIOS utilities.

   b. Before installing RHEL, set the date and time in the system BIOS.

2. Install RHEL manually.

   a. Select the language and keyboard layout for your region.

Some MCS software components depend on the language for RHEL being set to English. Please select English as the language of installation. Do not change the input language afterwards.

   b. When prompted to create storage, create three partitions on the OS drive:

   - sda1: Boot partition (/boot) - Required size: 512 MB
   - sda2: DRBD partition - Required size: 20 GB
   - sda3: System partition (/) - Suggested size: Remaining disk space

   c. When prompted, select the “Basic Server” and “Red Hat Enterprise Linux” options.

   d. Click the Reboot button to complete the installation.

3. Mount the RHEL installer:

   You must mount either the physical DVD or DVD.iso to the `/sysinstall` directory. This is where the MCS install script looks for it.

   If you have physical RHEL DVD media:

```
mount /dev/<device> /sysinstall
```

   In the above command, substitute <*device*> for the optical drive device name (e.g. sr0).

RHEL automatically creates an alias for the optical drive on /CDROM. Thus the following mount command can also be used: **`mount /CDROM /sysinstall`**

   If you have a RHEL .iso file:

   a. Create a directory on the server where you can copy the .iso. For example:

```
mkdir /media/RHEL
```

   For more information on mounting a USB drive, see “Copying Software to the MCS Server” on page 238.

   b. Copy the .iso to the newly created folder:

```
cp /path/rhel-server-6.5-x86_64-dvd.iso /media/RHEL
```

   c. Mount the .iso file:

```
mount -t iso9660 -o loop /media/RHEL/rhel-server-6.5-x86_64-dvd.iso /
sysinstall
```

In the above command, "*/media/RHEL*" is used as an example. Substitute "*/media/RHEL*" with the directory you created for the .iso.

4. Install MediaCentral Platform Services:
   a. Copy the MediaCentral Platform Services installation package to your server using your desired method.

      For more information on mounting a USB drive, see "Copying Software to the MCS Server" on page 238.

   b. If necessary, unzip the installation package:

      unzip MediaCentral_Services_*<version>*_*<build>*_Linux.zip

   c. Change directories to the MediaCentral_Services folder and run the installation script:

      ./install.sh

5. Once the installation is complete, follow the instructions in the body of this guide to complete the installation and configuration of MediaCentral Platform Services.

Working with the Dell RAID Controller

This section provides information for working with the Dell R620 / R630 RAID controller. The installation process assumes that the server shipped with preconfigured RAID 1 and RAID 5 arrays. If that is not the case, this information can be used to create the RAID sets.

Creating the RAIDs

To create the RAID1 and RAID5 arrays:

1. Enter the Dell RAID BIOS Utility.

   For more information, see "Dell PowerEdge R620 / R630 RAID Configuration" on page 55.

2. From the Virtual Disk Management menu, select Create Virtual Disk.

   If you just deleted the disk, this item is grayed-out. Go up one level in the menu system, and then return to the Virtual Disk Management page.

3. From the Create Virtual Disk page select Select Physical Disks.
4. Put check marks in the appropriate Physical Disk boxes.
   - For the RAID 1 (system disk) this should be 00:01:00 and 00:01:01
   - For the RAID 5 (optional cache disk) this should be 00:01:02 through 00:01:07.
5. Select Apply Changes.

   A confirmation screen indicates success.

6. From the Create Virtual Disk Page, select Create Virtual Disk.

   You may need to scroll down the page to see the link.

7. From the Warning page, confirm you selection and select Yes.

   A confirmation screen indicates success.

8. Return to the Virtual Disk Management page and select View Disk Group Properties to view your changes.

   You should see a Virtual Disk 0 (the RAID 1) and a Virtual Disk 1 (the RAID 5).

9. Return to the Integrated RAID Controller Configuration Utility page.
10. From the Integrated RAID Controller Configuration Utility menu choose Controller Management.
11. From the Controller Management menu choose Change Controller Properties.
12. Verify that the Virtual Disk 0 (the RAID 1) is selected in Set Bootable Device.

    If not, select it and apply your changes. Once you install RHEL and MCS, you want the server to boot from the RAID 1.
13. Exit the RAID configuration utility and return to the System Setup menu.

Deleting the RAIDs

If necessary, it is possible to delete the RAID sets from within the RAID controller.

To delete the RAID1 or RAID5 arrays:

1. From the Virtual Disk Management menu select Select Virtual Disk Operations.
2. Select the virtual disk of interest (the RAID 1 or RAID 5) from the drop-down menu.
3. Select Delete Virtual Disk.
4. Confirm your action.

   The menu indicates the success of the operation.

Card Placement in MCS Servers

Some installations might require the addition of an add-in PCIe card such as a Myricom 10GigE adapter which enables 10Gb network connection to the server. If your server requires additional hardware, review the following sections for card placement information.

The Myricom card ships with both a half-height and full-height bracket. Depending on which slot is used, you might need to replace the bracket when adding the card to the server.

Dell PowerEdge R620 and R630

The Dell PowerEdge R620 includes either 2 or 3 PCIe slots, depending on the configuration of the server. The Myricom 10GigE card can be added to any of the available slots. For consistency, Avid recommends using the top-left slot.

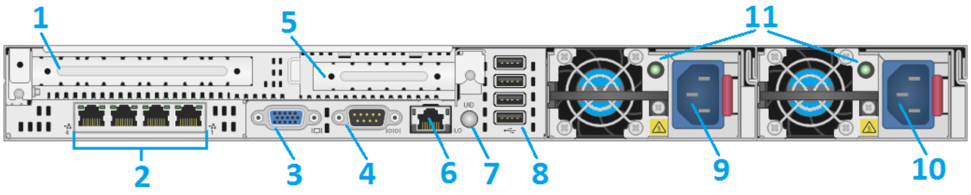
The Dell PowerEdge R630 includes 3 PCIe half-height slots. The Myricom 10GigE card can be added to any of the available slots. For consistency, Avid recommends using the top-left slot

HP ProLiant DL360 Gen9

The HP ProLiant DL360 Gen9 is equipped with one full height PCIe slots and two half-height slots. The Myricom 10GigE card can be added to any of the available slots. For consistency, Avid recommends using the top-left slot

HP ProLiant DL360p Gen8

The DL360p Gen8 has two PCIe slots and one Flexible LOM “slot”. The Flexible LOM is a clip-on board that connects directly to the motherboard.



1. PCIe 3.0 Full-height / half-length x16 expansion slot (Myricom 10 Gb / HP NC365T 1 Gb NIC card goes here)
2. Flexible LOM ports (Shown: 4 ports 1 Gb each)
3. Video connector
4. Serial connector
5. PCIe 3.0 Low Profile x8 expansion slot (not used)
6. iLO Management Engine NIC connector
7. Unit ID LED/button
8. Four USB connectors
9. Power supply bay 2 (Shown populated: Optional Power Supply for Redundant Power)
10. Power supply bay 1 (Primary Power Supply)
11. Power Supplies Health/Activity Indicators

Connecting to Avid Shared Storage

The HP DL360p Gen8 supports three possible connections to Avid Shared Storage:

- Myricom 10GigE
- HP NC365T 4-port GigE NIC
- HP 366FLR 4-port GigE NIC

If using either the Myricom or the HP NC365T network adapter, the card must be places in the full-height PCIe slot in the upper-left corner of the server (slot 1 as shown in the image above).

If ordered with the server, the HP 366FLR network adapter is located in the Flexible LOM slot.

Connecting to Non-Avid Storage

Interplay MAM deployments, where browse proxies reside on non-Avid storage, do not require additional NIC cards. They make use of the Ethernet ports built in to the HP server through the Flexible LOM slot. Visually verify that one of the built-in ports is connected to the network. For a 10GigE connection to non-Avid storage, use a 10GigE NIC of your choosing.

If MAM browse proxies reside on an Avid shared storage, the connection must be over a Zone 1, Zone 2, or Zone 3 (recommended) connection, using a supported GigE or 10GigE network interface.

Port Requirements

For information relating to network ports used with MediaCentral Platform Services, see the *Avid Networking Port Usage Guide* on the Avid Knowledge Base.

Direct link: http://avid.force.com/pkb/articles/en_US/readme/Avid-Networking-Port-Usage-Guide

Enabling Trusted Certificates

For security, MediaCentral Platform Services uses the Secure Sockets Layer (SSL) for its server-to-browser connections. This is indicated by an “s” in the “https://” address found in the browser’s address bar. Some browsers might also show a locked padlock icon for an SSL connection. SSL enables the secure transmission of information between web servers and web browsers.

For more information on configuring SSL certificates, see the Avid Knowledge Base:

http://avid.force.com/pkb/articles/en_US/how_to/SSL-Certificates-for-server-to-browser-connections

Contents of the MCS Installation Package

The MCS installation package, `MediaCentral_Services_<version>_Linux.zip`, is delivered as a compressed .zip file. The package includes the following:

Item	Description
MediaCentral_Services _*<version>*_Linux.tar.gz	The MCS Server Installation package. This compressed tar file contains numerous files, including the following useful shell script: `ics_version.sh` Once MCS is installed, a symlink is created and you can simply type the following to execute the script: **`ics_version`** For more information on this script, see "Determining the Installed MCS Version" on page 247.
install.sh	The installation script, for upgrades and installations.
iso2usb.exe, iso2usb.patch iso2usb_LICENSE.html iso2usb_README.rtf	Used in creating the MCS installation MCS Installation USB Drive.
system-backup.sh	Prepares for an upgrade by backing up important data, including system settings, network settings, the application.properties file, the UMS database, and more.

For the precise installation package name, see the *Avid MediaCentral Platform Services ReadMe*.

Determining the Installed MCS Version

The version and build numbers of the MCS installation can be verified with the following command:

```
ics_version
```

Version and build numbers are returned as follows:

```
Copyright 2014-2016 by Avid Technology, Inc.
System ID:

MediaCentral Services:
UMS          Version: x.x.x.x
ICPS         Version: x.x.x.x
ICPS manager Version: x.x.x.x
ACS          Version: x.x.x.x

<system type>

ICS installer: 2.9 (Build xx)
Created on <installer creation date>
```

Starting with MCS v2.6, if Media |Distribute, MAM Connector or other services are installed, version information on those components is also included in the output:

```
Media Distribute Services:
ServiceMix          Version: x.x.x
MPD                 Version: x.x.x
MPD UI              Version: x.x.x

MAM Connector       Version: x.x.x

Close Captioning    Version: x.x.x

Customizable logger Version: x.x.x

Assignments         Version: x.x.x
```

Some notes on the output:

- The System ID is an 11-digit number used in support calls, entered during system configuration.
- UMS - User Management Service
- ICPS - MediaCentral Playback Services
- ICPS manager - MediaCentral Playback Services Manager (player-to-server connection manager)
- ACS - Avid Common Services bus ("the bus")
- The <*system type*> indicates if this is a standalone server or if this server is part of a clustered configuration. If the server is part of a cluster, the nodes's status and Cluster IP is also displayed. For example:

  ```
  This is a Clustered system. Master node.
  The cluster IP is: 192.168.10.51
  ```

- If your system is part of a multi-zone configuration, the server's zone status is displayed as well as limited Media | Index configuration information. For example:

  ```
  Multi-Zone: Slave
  Media | Index configured: no
  ```

- ICS Installer - MediaCentral installer version and build number

For precise version numbers, see the *Avid MediaCentral Platform Services ReadMe*.

Using the MediaCentral Health Check Script

MediaCentral Platform Services v2.7 and later includes a script which enables users to quickly gather a wide range of valuable system information through a single command. When working with Avid Customer Care, this data is used in the troubleshooting process to help expedite solutions.

When running the utility, the following information is collected:

- Network information (host name, IP address, active network adapters, etc)
- Installed RHEL Security Updates
- RabbitMQ bus status
- Memory statistics
- Volume mounts, including Avid shared storage information
- Time synchronization information
- And much, more…

The script analyzes the system and collects data based on the server configuration. Clustered nodes report additional data on cluster-specific services such as Gluster and DRBD.

There are three ways to launch the health check:

- Running the script with no options collects the most communally requested set of data to troubleshoot issues with Avid Customer Care. Example:

  ```
  avid-system-check
  ```

- When the "-c" option is used, additional information such as low-level processes is collected which might be useful when troubleshooting specific issues. Example:

  ```
  avid-system-check -c
  ```

- The "-h" option displays the script's help page. Example:

  ```
  avid-system-check -h
  ```

Once the script is complete, a `<server_name>_health.txt` file is created and delivered to one or more e-mail addresses that are specified by the user who launches the script.

To run the Health Check script:

1. Log in to the MCS single-server or cluster master node as the Linux *root* user.

   For help identifying the master node, see "Identifying the Master, Slave and Load-Balancing Nodes" on page 268.

2. Launch the health check script by entering the following command:

   ```
   avid-system-check
   ```

   The script is located at `/opt/avid/bin/`, but it can be launched at any time regardless of the current directory.

3. The script will prompt you to enter one or more e-mail addresses where the health check text file will be sent. Enter any required addresses and press the Enter key.

   Multiple addresses must be separated by a single space. If you do not want the text file e-mailed to any address, press the Enter key to bypass this step.

   A "Working…" message appears on the screen. The script takes a few moments to complete and no indication of progress is displayed during the process.

   During this time, the script creates the `<server_name>_health.txt` file and e-mails it to all specified address(es). The Sender is listed as "root@<*MCS_server_hostname*>.localdomain" and the subject of the e-mail is "Avid MediaCentral Health-Check for <*MCS_server_hostname*>".

   Once the text file has been delivered, it can be viewed through any text editor. One such editor is Notepad++ which presents logs through an organized line-item display.

   Notepad++ can be downloaded from: https://notepad-plus-plus.org/

4. Once complete, the script asks if you wish to view the results on-screen.

   Type "**y**" to view the results or press any other key to exit the script.

To check for installed RHEL Security Updates

▶ The health-check script includes information about all installed RHEL security updates. This information is delivered by another smaller script called "avid-security-check". If a user is only interested in obtaining information about the security updates, the script can be run directly:

```
avid-security-check
```

Enabling the Player Demonstration Web Page

The player demonstration web page (https://<*host-domain*>/player/index.html) is a powerful tool for verification and troubleshooting. However, since it is accessible by way of an unrestricted URL, it is not installed by default (as of ICS 1.6).

The player demonstration web page is accessible by way of an unrestricted URL. This may be considered a security concern at customer sites. Moving or renaming its index.html file will prevent loading of the page. When not in use, move the player demonstration index.html file to a folder not accessible through https, such as the root user home directory (/root). The root user home directory is visible only to the root user. This is not to be confused with the root directory (/), which is visible to all users.

To install the player demonstration web page:

1. Log in to the MediaCentral single-server or cluster master node as the Linux root user.

   For help identifying the master node, see "Identifying the Master, Slave and Load-Balancing Nodes" on page 268.

2. Determine the name of the maxcut-devel RPM file containing the player demonstration web page:

   ```
   ls /opt/avid/Packages/
   ```

3. Manually install the maxcut-devel RPM:

   ```
   rpm -ivh /opt/avid/Packages/maxcut-devel-<version>-<build>.x86_64.rpm
   ```

   The system responds indicating the success of the installation.

4. To verify the package has been installed:

   ```
   rpm -qa | grep max
   ```

5. Log in to the slave node as root and repeat the process.

6. To launch the player demo web page by opening a browser and navigating to the following URL:

   https://<*host-domain*>/player/index.html

   Where <*host-domain*> is the host name or FQDN of the node where you installed the player demonstration page. For a cluster, enter the virtual host name of the cluster instead.

To move the player demonstration web page to a secure location:

1. Enter the following command:

   ```
   mv /var/www/html/player/index.html /root
   ```

If you wish to uninstall the player demonstration page, enter the following command:

```
rpm –e maxcut-devel
```

Verifying Cache Directory Permissions

As part of the installation process, a number of cache directories are created and directory ownership and permissions are set. In this section, you verify that the permissions are set correctly.

This procedure is only necessary for cluster deployments. Do not use this procedure for a single node deployment. Some directories might not be present, as they are created automatically during operation of the system. Adjust the steps accordingly.

To verify cache directory permissions:

1. Verify the ownership and permissions for of all cache directories:

   `ls -la /cache`

   The command returns information similar to the following:

   ```
   drwxrwxrwx 9 maxmin maxmin 4096  Sep 3 14:30 .
   dr-xr-xr-x33 root   root   4096  Sep 3 13:59 ..
   drwxrwsrwx 2 maxmin maxmin 4096  Sep 3 16:03 download
   drwxrwsrwx 2 maxmin maxmin 4096  Sep 3 16:03 fl_cache
   drwxr-xr-x 5 root   root   4096  Sep 3 17:02 gluster
   drwx------ 2 root   root   16384 Sep 3 16:00 lost+found
   drwxrwxrwx 2 root   root   4096  Sep 3 14:29 mob-fetch
   drwxr-xr-x 2 root   root   4096  Sep 3 14:30 render
   drwxrwxrwx 9 root   root   4096  Sep 3 16:17 spooler
   ```

   Note that in the output above the dot (".") directory represents the current directory, that is, `/cache`.

   Note that some directories might not exist yet, as explained in the following table:

Directory	Description
`/cache/fl_cache`	Automatically created and assigned maxmin ownership by MCS processes only after specific media types have been accessed.
`/cache/download`	Same as above.
`/cache/render`	Automatically created by MCS processes with first multicam playback.

2. The following directories must be owned by user maxmin:

   `/cache`

   `/cache/download`

   `/cache/fl_cache`

3. The following directories must have the SGID (Set Group ID) special bit set:

   `/cache/download`

   `/cache/fl_cache`

   The SGID bit is shown as an "s" in the permissions list: `drwxrwsrwx`

4. If the ownership and permissions are not set correctly, refer to "Making the RHEL Cache Directories" and "Changing Ownership and Mounting the GlusterFS Volumes" in the *MediaCentral Platform Services Installation and Configuration Guide Version 2.4*.

Modifying application.properties

The application.properties file can be altered to add custom modifications that might be desired for some MCS installations. This section includes where to find and how to customize the file to suit your site's needs.

Editing the File

The following process details how to open and edit the application.properties file for editing. Refer to the Configuration Changes section for information on making specific changes to the file.

To edit the application.properties file:

1. Log in to the MCS server as the 'root' user. If you have a clustered configuration, log into the master node.
2. Enter the following command to navigate to the directory containing the file:

   ```
   cd /opt/avid/etc/avid/avid-interplay-central/config
   ```

3. This directory contains an "application.properties.example" file. The example file includes information on some features that can be adjusted. If "application.properties" does not already exist, use the following command to rename this file to exclude the ".example" extension:

   ```
   mv application.properties.example application.properties
   ```

4. Edit the file using a text editor (such as vi):

   ```
   vi application.properties
   ```

5. Add the required text to the end of the file.

   See the Configuration Changes section below for possible options.

6. Save and exit the vi session. Press <ESC> and type: `:wq`
7. (Cluster configurations only) Repeat steps 1 – 6 on the slave node.
8. Once complete, the avid-interplay-central service must be restarted.

This step will disconnect any users currently working on the system.

- If running a single server configuration:

  ```
  service avid-interplay-central restart
  ```

- If running a clustered configuration, the avid-interplay-central service is restarted through the AvidIPC cluster resource. Issue following command from any node in the cluster:

  ```
  crm resource restart AvidIPC
  ```

Configuration Changes

The following is a list of optional items that can be added to application.properties. Each of these adjustments will modify the default behavior of MediaCentral Platform Services.

To Disable Desktop Notifications

MCS v2.4 introduced the ability to show notifications from a web browser when certain actions are completed in MediaCentral UX. This feature can be disabled for all clients by adding the following line to application.properties:

```
system.client.desktopNotifications.enabled=false
```

See the *Avid MediaCentral | UX User's Guide* for more information on this feature.

To Adjust Load Balancing Communication

When a playback request is received by MCS, the system returns the FQDN of the cluster during the load-balancing handshake. To avoid issues with DNS, some networks benefit from altering this configuration to return the cluster's virtual IP address instead of the FQDN. To make this change, add the following line to application.properties:

```
system.com.avid.central.services.morpheus.media.UseIpForPreferredHost=true
```

For more information, see "Validating the FQDN for External Access" on page 161.

To Add Passwords for SSL Certificates

For security, MediaCentral Platform Services uses the Secure Sockets Layer (SSL) for its server-to-browser connections. SSL enables the secure transmission of information between web servers and web browsers. In MediaCentral v2.4 and earlier, the application.properties file is altered when configuring the SSL password. MediaCentral v2.5 and later uses a different process for creating the SSL certificates that does not involve altering the application.properties file.

For more information, see the article on configuring SSL Certificates on the Avid Knowledge Base:

http://avid.force.com/pkb/articles/en_US/how_to/SSL-Certificates-for-server-to-browser-connections

To Adjust the Default Audio Panning

The default audio panning for advanced sequences is: odd tracks=left, even tracks=right. To override this panning, add the following line to application.properties:

```
system.advancedSequenceTrackPanning=<values>
```

Where <*values*> uses the following syntax:

- Key=value pairs separated by a semicolon. For example, A1:R;A2:C.
- Keys need to be in this set: A1, A2, A3, A4, A5. Not all need to be added; only keys for the tracks that you want to override. Advanced sequences have a maximum of five tracks.
- Values can be R, r, Right, right, L, l, left, Left, C, c, Center, center

For example:

```
system.advancedSequenceTrackPanning=A1:R;A2:C;A5:Right;
```

You can use this procedure to set panning for STP stereo mixdown as it was in MediaCentral v2.0. In v2.0, single-channel tracks were mixed down to a single centered mono track. In v2.1, they are mixed left or right by default. To preserve the v2.0 behavior, edit the application.properties file with this key:

```
system.advancedSequenceTrackPanning=A1:C;A2:C;A3:C;A4:C;A5:C;
```

To Disable Client Logging

Log messages pertaining to the client application can be found on the MCS server at: `/var/log/avid/avid-interplay-central/`. If desired, this logging can be disabled by adding the following line to application.properties:

```
system.clientLoggingEnabled=false
```

To Adjust the Default Search Type

MCS systems configured for Media Index have two search types available: federated and indexed. By default, the Search bar and the Search pane in MediaCentral UX use the federated search, and indexed searches use the simple search syntax. You can specify the default search type and search syntax by adding the following lines to application.properties.

- To set the default search for all search panes in MediaCentral UX as the indexed search:

  ```
  system.client.search.default=Indexed
  ```

  By default this value is set to "Federated."

- To set the default search used in the Search bar as the indexed search:

  ```
  system.client.search.quicksearch.default=Indexed
  ```

  By default this value is set to "Federated."

- To set all indexed searches to use Advanced search syntax as the default search syntax:

  ```
  system.client.search.advanced_as_default=true
  ```

See the *Avid Media Index Configuration Guide* for more information on this feature.

To Detect Black Gaps in Video Sent to Playback

A user might unintentionally include gaps in the video track that result in black gaps in the video output. This could cause a problem when the sequence is sent to playback. MediaCentral UX v2.1.2 and later includes an option to check a sequence for gaps in the video. If the system detects a gap, one of the following actions are taken, depending on how this option is configured:

- none: No message is displayed and the sequence is sent to the playback device.
- warning: A warning message is displayed and the user can either continue the operation or cancel it.
- error: An error message is displayed and the process is canceled.

After viewing the warning or error, the user can edit the sequence to remove the gaps and retry the STP operation.

This feature applies only to advanced sequences.

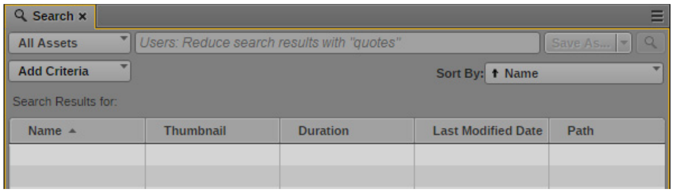
To make this change, add the following line to application.properties:

```
system.client.stp.video-gap-warning=warning
```

Substitute ERROR for WARNING if you want an error message that cancels the operation. Substitute NONE if you do not want any message.

To Enable Custom Text in the Search Field

The MediaCentral UX Search field displays a default message of "Enter search text here" which provides users direction for using the search. If desired, Administrators can replace the default message with custom data which appears in the search field as light gray text. In the following example, *"Users: Reduce search results with "quotes""* has replaced the default message:



When a user begins to enter text in the search field, the message is replaced by the user's search criteria.

To enable a custom message, enter the following line to the application.properties file:

```
system.client.search.indexed.placeholder=<value>
```

<*value*> represents a custom message.

To Enable Auto-population of the STP Video ID Field

System administrators have the option to adjust a setting on the MCS servers to automatically populate the Video ID field in the Send To Playback window with the sequence name. Once populated, users can alter the Video ID field with a custom value if desired.

If the sequence has already been assigned a Video ID through the MediaCentral UX Metadata pane or through an external system such as Avid iNEWS, the ID does not change and the text area cannot be edited.

To make this change, add the following line to application.properties:

```
system.client.stp.automatically-set-videoid-to-name=true
```

Specifying the RabbitMQ Network Adapter

In some environments, the MCS server might have more than one enabled network adapter. In these situations, the second network adapter might be connected to a network that has indirect or no access to the rest of the production environment. By default RabbitMQ prefers the network device with the label “eth0”. If that adapter is unavailable, the service uses any network device which is in the “UP” state. The avid-acs-gateway service uses the IP address returned by the “avid-rmq-discovery” plug-in to connect to RabbitMQ. If the wrong IP address is supplied to the gateway, communication issues can occur.

To ensure that the service uses the correct network adapter at all times, you must edit a RabbitMQ configuration file. This process applies to both single-server and Corosync cluster configurations that have a second enabled network adapter.

If you are configuring a new installation, see “Configuring RabbitMQ for a New Installation” on page 256.

If you are adding adjusting the configuration on an existing installation, see “Configuring RabbitMQ for an Existing Installation” on page 257.

If a future version of MediaCentral Platform Services requires a change to this file, a .newrpm file is crated in the /sysconfig directory. The adjustments described in the process below must be manually migrated to the new file. For more information on making manual adjustments, see “Verifying System Configuration Files” in the Avid MediaCentral Platform Services Upgrade Guide.

Configuring RabbitMQ for a New Installation

In an new installation, users are directed to adjust the RabbitMQ network adapter early in the MCS installation and configuration process. In a cluster configuration, the following process must be completed on each node, before the systems are clustered.

To configure the RabbitMQ network adapter for a new installation:

1. Log into the MCS server (at the Linux prompt) as the root user.
2. Open the `avid-rmq-discovery-plugin` configuration file with a text editor (such as vi):

   ```
   vi /etc/sysconfig/avid-rmq-discovery-plugin
   ```

3. Remove the “#” symbol in front of the 'RMQ_NIC_LABEL' parameter and enter the name of your primary network adapter. For example to specify “eth0”, you would enter the following:

   ```
   RMQ_NIC_LABEL=eth1
   ```

Alternatively, system administrators can associate a specific IP address with RabbitMQ by changing the METHOD value to “manual” and the RMQ_IP_ADDR value to the IP address assigned to the network adapter. For example:

```
METHOD=manual
RMQ_IP_ADDR=192.168.10.51
```

If you alter the METHOD and RMQ_IP_ADDR values, do not also alter the RMQ_NIC_LABEL value.

4. Save and exit the vi session. Press <ESC> and type: **:wq**

5. Once the configuration file has been saved, restart the rabbitmq-server service to enable the change:

   ```
   service rabbitmq-server restart
   ```

   The command should report the following:

   ```
   [root@wavd-mcs01 ~]# service rabbitmq-server restart
   Stopping rabbitmq-server:                                  [  OK  ]
   Starting rabbitmq-server:                                  [  OK  ]
   ```

   Verify that the service starts and reports a status of OK.

6. Once the changes are complete and the service has been restarted, you can verify your settings with the following command:

   ```
   acs-broker-discovery
   ```

   You will see output similar to the following:

   ```
   status  ip              node            az
   ok      10.106.10.51    wavd-mcs01      MCS
   ```

   The Availability Zone (az) should always report “MCS”.

   If you are building a cluster, repeat this command on each node.

7. Restart the avid-acs-gateway service to ensure the correct network adapter is used:

   ```
   service avid-acs-gateway restart
   ```

8. If you are configuring a cluster, repeat the above steps on all cluster nodes.

Configuring RabbitMQ for an Existing Installation

If you are adding a second network adapter to an existing installation, the process to configure the network adapter for a single server is the same as the process for a new installation. However in a cluster configuration, special care must be taken to restart the rabbitmq-server service to ensure no loss of RabbitMQ queue data. See the process below for more information.

To configure the RabbitMQ network adapter for an existing cluster installation:

1. Complete steps 1 - 4 for “Configuring RabbitMQ for a New Installation” on page 256.

2. Starting with the Corosync master node, restart the rabbitmq-server service:

   ```
   service rabbitmq-server restart
   ```

   The command should report the following:

   ```
   [root@wavd-mcs01 ~]# service rabbitmq-server restart
   Stopping rabbitmq-server:                                  [  OK  ]
   Starting rabbitmq-server:                                  [  OK  ]
   ```

   Verify that the service starts and reports a status of OK.

3. Continue to restarting the service on the slave node and any load-balancing nodes. Complete this step one node at a time, always verifying that an OK status is reported before moving on to the next node.

4. Restart the avid-acs-gateway service to ensure the correct network adapter is used:

   - For a single server, use the following command:

     ```
     service avid-acs-gateway restart
     ```

- For a cluster configuration, restart the cluster resource that manages the avid-acs-gateway service. This command can be issued from any node:

  ```
  crm resource restart AvidGateway
  ```

5. Once the changes are complete and the service has been restarted, you can verify your settings with the following command:

   ```
   acs-broker-discovery
   ```

   You will see output similar to the following:

   ```
   status  ip              node            az
   ok      10.106.10.51    wavd-mcs01      MCS
   ok      10.106.10.52    wavd-mcs02      MCS
   ok      10.106.10.53    wavd-mcs03      MCS
   ```

   The Availability Zone (az) should always report “MCS”.

   If a failure has occurred, an error appears in the output of this command. For example:

   ```
   status  ip              node            az
   error   10.106.10.51    wavd-mcs01      MCS
   ok      10.106.10.52    wavd-mcs02      MCS
   ok      10.106.10.53    wavd-mcs03      MCS

   [ERROR] Node request failed:
   Error: connect ECONNREFUSED 10.106.77.199:15672
   ```

   If an error occurs, verify the changes you made to the `avid-rmq-discovery-plugin` and if necessary, restart the service again on the problem node.

6. Verify the status of the RabbitMQ service:

   ```
   service rabbitmq-server status
   ```

   The command will return a detailed string of data regarding the service. Example (partial only):

   ```
   [root@mcs-1 ~]# service rabbitmq-server status
   Status of node 'rabbit@mcs-1' ...

   [{pid,2064},
    {running_applications,
        [{rabbitmq_federation_management,"RabbitMQ Federation Management",
             "3.3.5"},
         {rabbitmq_management,"RabbitMQ Management Console","3.3.5"},
   ```

   Review the output of the command and verify there are no obvious error messages such as “`service is dead but pid (xxxxx) is running`”.

7. Check the RabbitMQ cluster with the “rabbitmqctl cluster_status” command:

   ```
   rabbitmqctl cluster_status
   ```

   The following is an example of a 2-node cluster:

   ```
   Cluster status of node 'rabbit@node-n1’ ...
   [{nodes,[{disc,['rabbit@node-n1','rabbit@node-n2']}]},
   {running_nodes,[ 'rabbit@node-n1','rabbit@node-n2']},
   {cluster_name,<<"rabbit@node-n1">>},
   {partitions,[]}]
   ```

   The command should return information about each of the RabbitMQ cluster nodes. All available nodes should appear on both the “nodes” and “running_nodes” lines.

   Verify that each node reports the same information about the RabbitMQ cluster (all nodes are known and running).

Working with the MediaCentral UX Configurator

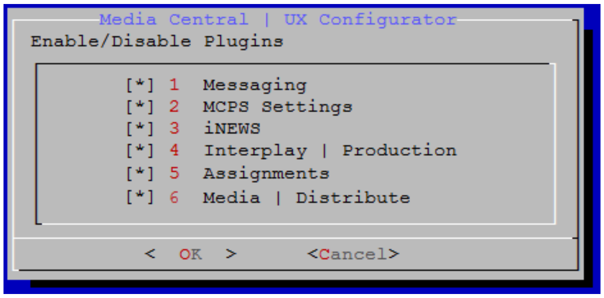
Located at `/opt/avid/avid-interplay-central/configurator`, the MediaCentral UX Configurator enables or disables functionality available in MediaCentral UX. The standard features that appear in the tool are:

- Messaging
- MCPS Settings
- iNEWS
- Interplay | Production

Additional features that could appears in the Configurator:

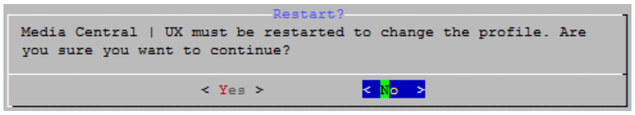
- Assignments
- MaestroUX
- MaestroAssetBrowser
- Media | Distribute

Each of the standard features are enabled by default when MediaCentral Platform Services are installed. Additional features might also appear in the Configurator. However, these features only appear after additional software has been installed on the MCS server. The following image indicates that both Assignments and Media Distribute have been installed on the server:



```
Media Central | UX Configurator
Enable/Disable Plugins

        [*] 1  Messaging
        [*] 2  MCPS Settings
        [*] 3  iNEWS
        [*] 4  Interplay | Production
        [*] 5  Assignments
        [*] 6  Media | Distribute

        <  OK  >        <Cancel>
```

When enabling or disabling a feature, the following window appears after selecting OK:



```
Restart?
Media Central | UX must be restarted to change the profile. Are
you sure you want to continue?

                < Yes >         < No  >
```

If you select **No**, the tool exits without restarting the avid-interplay-central service. Configuration changes are not enabled until the next restart of the service or cluster resource.

If you select **Yes**, the avid-interplay-central service is restarted:

```
Avid Interplay Central process has been started.
Wait for Interplay Central web interface...
Avid Interplay Central has been started successfully (36 seconds)
```

Restarting the avid-interplay-central service disconnects any users currently logged into the system. If you need to make changes to the Configurator options, it is advised to do so during a maintenance window.

If you are running the Configurator on a clustered system, the tool only needs to be run on the master and slave nodes as these are the only nodes in the cluster that will run the AvidIPC resource. As a reminder, the AvidIPC resource manages the avid-interplay-central service.

The Configurator tool is not cluster-aware, so special care needs to be taken on clustered systems. When making a change through the Configurator on a functional cluster, complete the following:

To run the Configurator tool:

1. Run the Configurator on the master node.
2. Make the required changes and select OK.
3. When you are presented with the window asking if you want to continue, select **`No`**.

   In a cluster, the AvidIPC resource manages the avid-interplay-central service. If the service is restarted, the cluster will see this as a failure and will increase the fail-count of the service which could lead to a fail-over event.
4. Repeat steps 1 – 3 on the slave node.
5. Once the change has been made on both nodes, restart the AvidIPC resource:

   ```
   crm resource restart AvidIPC
   ```

Backing up and Restoring the MCS Database

You may recall that the system-backup script, discussed in the Backing up and Restoring the MCS System Settings and Database section of this document, calls the avid-db command as part of its system setting backup process.

The MCS database is automatically backed up by the same avid-db utility on a daily basis. If desired the utility can run manually to back up and restore the database (plus perform other operations) at any time.

The avid-db command has the following format:

```
/opt/avid/bin/avid-db <parameter-list> <command> [ <args>... ]
```

For example, to back up the contents of the MCS database to `/opt/avid/share/avid/db/dumps`:

```
/opt/avid/bin/avid-db --dump-base=/opt/avid/share/avid/db/dumps dumpall
```

For a list of all the parameters and arguments, issue the following:

```
/opt/avid/bin/avid-db help
```

Restoring the MCS database in cluster has special requirements. Due to the automatic restarting of halted services in a cluster, do not use the avid-db restore command by itself. Follow the procedure as outlined below.

To restore the MCS database in a cluster:

1. Log in to the master and slave nodes as root.

   For help identifying the node, see "Identifying the Master, Slave and Load-Balancing Nodes" on page 268.

2. Stop pacemaker on the slave node:

   ```
   service pacemaker stop
   ```

3. Stop pacemaker on the master node:

   ```
   service pacemaker stop
   ```

4. Start DRBD on the master node:

   ```
   service drbd start
   ```

5. Start DRBD on the slave node:

   ```
   service drbd start
   ```

6. Run the following command on the master node to make it the DRBD primary:

   ```
   drbdadm primary r0
   ```

7. Mount the DRBD drive on the master node:

   ```
   mount /dev/drbd1 /mnt/drbd
   ```

8. Start the PostgreSQL database on the master node:

   ```
   service postgresql-9.1 start
   ```

9. Restore the MCS database on the master node:

   ```
   /opt/avid/bin/avid-db --drop-db="no" restoreall
   ```

   Once the MCS database has been restored, begin handing control back to pacemaker in the steps below.

10. Stop PostgreSQL on the master node:

    ```
    service postgresql-9.1 stop
    ```

11. Unmount the DRBD drive on the master node:

    ```
    umount /mnt/drbd
    ```

12. Stop DRBD on both nodes:

    ```
    service drbd stop
    ```

13. Restart Pacemaker (which restarts all needed services) on both nodes, master node first, slave node second:

    ```
    service pacemaker start
    ```

    This command brings all cluster resources back online.

14. Use the Cluster Resource Monitor to verify that all resources have started and that all nodes are online:

    ```
    crm_mon -f
    ```

    For more information on using the Cluster Resource Monitor, see the "Cluster Resource Monitor" chapter of the *MediaCentral Platform Services Concepts and Clustering Guide*.

Working with the Avid Shared Storage Client

The following concepts in this section apply to Avid shared storage:

- Verifying the Avid Shared Storage Mount
- Reconfiguring the Avid Shared Storage Connection
- Downgrading the Avid Shared Storage Client

Verifying the Avid Shared Storage Mount

The connection to Avid shared storage is initially verified during the MediaCentral UX System Settings configuration process. In that procedure, the Status of the connection changes from “Disconnected” to “Connected”.

However, it is possible to verify the storage mounts using various command line tools which can be useful for troubleshooting. Examples of such commands are:

- **`service avid-isis status`**
- **`mount -t fuse.avidfos`**
- **`df -h`**

To verify the Avid shared storage mount(s):

1. Verify the status of the avid-isis service (used for both Avid ISIS and Avid NEXIS):

   ```
   service avid-isis status
   ```

   The system responds with output similar to the following:

   ```
   AVID Service: isis fuse_avidfos (pid  2302) is running...[  OK  ]
   ```

2. Use the Linux mount command to display all mounted file systems of type fuse.avidfos (the Avid shared storage file system):

   ```
   mount -t fuse.avidfos
   ```

   The system responds with output showing the storage mount, similar to the following:

   ```
   wavd-isis on /mnt/ICS_Avid_Isis/wavd-isis type fuse.avidfos
   (rw,nosuid,nodev,allow_other,default_permissions)
   ```

   The output above indicates that an Avid shared storage system named “wavd-isis” is mounted at `/isis/wavd-isis`. “Fuse” is the RHEL file system type reserved for third-party file systems.

3. The Linux `df` command displays disk usage information for all the mounted file systems:

   ```
   df -h
   ```

   The system responds with output similar to the following:

   ```
   Filesystem            Size  Used Avail Use% Mounted on
   /dev/mapper/vg_icps-lv_cache
                         527G  6.3G  494G   2% /
   tmpfs                  24G     0   24G   0% /dev/shm
   /dev/sda1             485M   33M  428M   8% /boot
   wavd-isis              15T  5.7T  8.9T  40% /mnt/ICS_Avid_Isis/wavd-isis
   /dev/sdb1             7.3G  5.5G  1.9G  75% /media/usb
   ```

4. Finally, explore the mounted workspaces available to the MCPS player by navigating to the share(s) as you would any Linux file system:

   ```
   ls /mnt/ICS_Avid_Isis/<virtual system director>
   ```

   The command returns a list of workspaces available to the user defined in the “Playback Service” settings of the MediaCentral UX System Settings.

Reconfiguring the Avid Shared Storage Connection

During the initial MCS installation process, a single network interface is configured as the primary network adapter for the system. If at a later date, a different network adapter is required, the following process provides instructions for reconfiguring the system.

A common example of this situation is the addition of a 10Gb network card to replace a single 1Gb connection.

To reconfigure the network connection:

1. Install the new card.

   For details, see “Network Interface Cards and Network Connections” on page 19.

2. Verify the NIC interface names using the RHEL Network Configuration tool.

   For details, see “Identifying NIC Interfaces and Connecting the Network Cable” on page 69.

3. If running an HP server, swap the NIC interface names so the new card owns port eth0 by editing the 70 persistent net.rules file.

   For details, see “(HP Only) Swapping NIC Interface Names” on page 70.

4. If running an HP server, remove the MAC address hardware references for the swapped ports from the corresponding `ifcfg-ethX` files and reboot.

   For details, see “(HP Only) Removing the MAC Address Hardware References” on page 71.

5. Sign in to MediaCentral UX with administrator privileges and update the storage connection in the Playback Service System Settings to match the new connection speed.

   For example, change it from “1 Gb Connection” to “10 Gb Connection”.

   For details, see “Playback Service Settings” on page 100.

Downgrading the Avid Shared Storage Client

MediaCentral Platform Services includes both the Avid ISIS Client and the Avid NEXIS Client software. The ISIS Client is installed by default through the MCS installation or upgrade process. The NEXIS Client is simply bundled with the MCS software for convenience and is not actively installed.

The body of this guide includes instructions for upgrading the shared storage client software. If it becomes necessary for any reason, the following section details how to revert to an alternate version of the client.

To downgrade the shared storage client on a single server:

1. Verify the current version of the installed shared storage client software:

   ```
   rpm -qa | egrep -i 'isis|nexis'
   ```

   This command returns all installed packages with either ISIS or NEXIS in the name.

2. Stop the ICPS back-end services (the services that use the storage client):

   ```
   service avid-all stop
   ```

3. Run the following commands to replace the Avid NEXIS Client with the original Avid ISIS Client:

   ```
   rpm -e AvidNEXISClient
   ```

   ```
   rpm -Uvh /opt/avid/Packages/AvidISISClient-<version>.el6.x86_64.rpm
   ```

4. Check the version of the shared storage client and verify that it has changed:

   ```
   rpm -qa | egrep -i 'isis|nexis'
   ```

5. Restart the ICPS back-end services:

   ```
   service avid-all start
   ```

To downgrade the shared storage client in a cluster:

1. Verify the current version of the installed shared storage client software:

   ```
   rpm -qa | egrep -i 'isis|nexis'
   ```

   This command returns all installed packages with either ISIS or NEXIS in the name.

2. Before the client can be uninstalled, the cluster resource that uses the client must first be stopped:

   ```
   crm resource stop AvidAllEverywhere
   ```

   This single command will stop the resource for all cluster nodes.

3. Run the following commands to replace the Avid NEXIS Client with the original Avid ISIS Client:

   ```
   rpm -e AvidNEXISClient
   ```

   ```
   rpm -Uvh /opt/avid/Packages/AvidISISClient-<version>.el6.x86_64.rpm
   ```

   Repeat these commands on all cluster nodes, in any order.

4. Check the version of the shared storage client and verify that it has changed:

   ```
   rpm -qa | egrep -i 'isis|nexis'
   ```

   Repeat this command on all cluster nodes, in any order.

5. Once the client has been installed on all nodes, start the associated cluster resource:

   ```
   crm resource start AvidAllEverywhere
   ```

6. Open the Cluster Resource Monitor and verify that the resource starts correctly:

   ```
   crm_mon -f
   ```

7. If any fail-counts appear, clear them with the following command:

   ```
   crm resource cleanup <rsc> [<node>]
   ```

   - *<rsc>* is the resource name of interest: AvidIPC, AvidUMS, AvidACS, etc.
   - *<node>* (optional) is the node of interest. Omitting the node cleans up the resource on all nodes.

   Press CTRL-C on the keyboard to exit the Cluster Resource Monitor.

   For more information on using the Cluster Resource Monitor, see the “Cluster Resource Monitor” chapter of the *MediaCentral Platform Services Concepts and Clustering Guide*.

Additional information on Clustering

The following concepts in this section apply to MediaCentral Platform Services cluster configurations:

- Unicast Support in Clustering
- Reconfiguring MediaCentral Settings in a Cluster
- Taking a Cluster Node Off-Line Temporarily
- Identifying the Master, Slave and Load-Balancing Nodes

For more information on clustered configurations, see the *MediaCentral Platform Services Concepts and Clustering Guide*.

Unicast Support in Clustering

MCS clustering supports both unicast and multicast communication protocols. The default configuration, as set up by the cluster installation script (and covered in the body of this guide) uses multicast. In facilities where the network does not support multicast (the feature is not enabled), configuring the cluster for unicast communication is an alternative.

This process can also be used for new installations and for systems that already have a functional cluster configured for multicast and wish to convert to unicast communication.

Configuring a cluster for unicast requires altering the contents of the Corosync configuration (corosync.conf) file.

The following is an example of the default Corosync configuration file using multicast:

```
totem {
        version: 2
        secauth: off
        threads: 0
        interface {
                ringnumber: 0
                bindnetaddr: 192.168.10.0
                mcastaddr: 239.192.1.1
                mcastport: 5405
        }
}
```

The following is an example of an altered Corosync configuration file using unicast:

```
totem {
        version: 2
        secauth: off
        threads: 0
        interface {
            member {
                memberaddr: 192.168.10.51
            }
            member {
                memberaddr: 192.168.10.52
            }
            ringnumber: 0
        bindnetaddr: 192.168.10.0
        mcastport: 5405
    }
    transport: udpu
```

Note the following changes in the altered file:

- A “`member{}`” section for each node in the cluster has been added.
- “`mcastaddr: 239.192.1.1`” has been removed.
- A “`transport: udpu`” line has been added.

This process assumes that the following steps from the Clustering section of this guide have already been completed:

- Cluster Overview
- Configuring the Player System Setting
- Configuring DRBD

If you are converting an existing multicast cluster to unicast communication, skip Step 1 of the following process.

To configure unicast cluster communication:

1. Run the following command on each node in the cluster:

   ```
   /opt/avid/cluster/bin/cluster setup-corosync --corosync-bind-
   iface=interface --rabbitmq_master="master hostname"
   ```

   When using this command, reference the following:

   - *interface*: Identifies the name of the primary network interface. In an HP server, this is generally “eth0”. In a Dell server, this is generally “em1” for 1 Gb connections or “p1p1” / “p2p1” for 10 Gb connections (depending on which slot the card 10 Gb card has been installed). For Interplay MAM configurations with port bonding, this is generally “bond0”. Quotes are required with this variable.
   - *master hostname*: Specifies the (short) hostname of the Master node in the cluster (e.g. wavd-mcs01). This should be the same as the DRBD Master node specified in the `drbd_setup` process. Quotes are required with this variable.

The body of this guide instructs you to run this command on the master node only. In this process, you will run the command on all nodes.

2. Stop the cluster services on all load-balancing nodes:

   ```
   service pacemaker stop && service corosync stop
   ```

3. Stop the cluster services on the slave node:

   ```
   service pacemaker stop && service corosync stop
   ```

4. Open the Cluster Resource Monitor to verify that the slave and any load-balancing nodes appear as “OFFLINE”:

   ```
   crm_mon
   ```

   Press CTRL-C on the keyboard to exit the Cluster Resource Monitor.

5. Once the cluster services have been stopped on the slave node, stop the services on the master node:

   ```
   service pacemaker stop && service corosync stop
   ```

6. Using the example provided in this section as a guide, edit the Corosync configuration file:

   ```
   vi /etc/corosync/corosync.conf
   ```

   - Remove **mcastaddr** from the file (leave **mcastport**).
   - Add the new transport (that indicates unicast): **udpu**.
   - Create a **member{}** section for each node in the cluster, following the example, but replacing the values for **memberaddr** with the IP addresses of your own cluster nodes.

7. Restart the cluster services on the nodes in the reverse order that you stopped them (master node first, then slave, then load-balancing nodes):

   ```
   service corosync start && service pacemaker start
   ```

   Prior to starting the services on the slave and load-balancing nodes, use the Cluster Resource Monitor, crm_mon, to verify that all resources have started on the master node.

8. Once you have completed the above instructions on each node in the cluster, run the setup-cluster command on the DRBD master node only, following the instructions in the body of this guide. The most commonly used form of the setup-cluster command is provided below (for reference):

   ```
   /opt/avid/cluster/bin/cluster setup-cluster
   --cluster_ip="<cluster IP address>"
   --pingable_ip="<router IP address>"
   --cluster_ip_iface="<interface_name>”
   --admin_email="<comma separated e-mail list>"
   --drbd_exclude="<comma separated list of non-DRBD nodes>"
   ```

   For details (and the appropriate form of the setup-cluster command), see “Starting the Cluster Services on the Master Node” on page 124.

9. Restart the following services on each node so that they register correctly on the newly created instance of the message bus:

   ```
   service avid-acs-messenger restart
   ```

   ```
   service avid-aaf-gen restart
   ```

   ```
   service avid-acs-mail restart
   ```

10. Launch the Cluster Resource Monitor to verify that the cluster is aware of all nodes and that all services are running normally.

    ```
    crm_mon -f
    ```

    Press CTRL-C on the keyboard to exit the Cluster Resource Monitor.

    For more information on using the Cluster Resource Monitor, see the “Cluster Resource Monitor” chapter of the *MediaCentral Platform Services Concepts and Clustering Guide*.

Reconfiguring MediaCentral Settings in a Cluster

If you reconfigure any MediaCentral UX System Settings (e.g. adding/removing an Avid shared storage system), the new settings are retained by the master node only. Non-master nodes must be updated manually.

On each non-master node, log in as root and run the following command:

```
service avid-all reconfigure
```

Taking a Cluster Node Off-Line Temporarily

If you need to take a node offline make sure to alert users that playback might stop. In the best case, the client will automatically re-connect to one of the remaining available nodes, though it may take several seconds. In the worst case, the end-user be required to sign in to MediaCentral UX again, in which case playback will be stopped.

To take a cluster node off-line temporarily, log in as root on any node and issue the following command:

```
crm node standby <hostname>
```

In the above command, replace <*hostname*> with the name of the node to be brought off-line.

Identifying the Master, Slave and Load-Balancing Nodes

There are three types of nodes in a cluster: master, slave, and load-balancing. The master “owns” multiple resources such as the cluster IP address. The slave assumes the role of master in the event of a fail-over. Additional nodes play a load-balancing role, but can never take on the role of master.

To identify the master, slave, and load-balancing nodes:

1. Verify the current role of each node by logging in to any machine in the cluster as the root user and typing:

   ```
   crm_mon
   ```

2. To identify the master and slave nodes, look for the line containing “Master/Slave Set”.

   For example:

   ```
   Master/Slave Set: ms_drbd_postgres [drbd_postgres]
   Masters: [ wavd-mcs01 ]
   Slaves: [ wavd-mcs02 ]
   ```

   In this example, the master node is wavd-mcs01 and the slave node is wavd-mcs02.

3. To identify the load-balancing nodes, look for the line containing “Clone Set”.

   For example, if the crm_mon command output contains the lines:

   ```
   Clone Set: AvidAllEverywhere [AvidAll]
   Started: [ wavd-mcs01 wavd-mcs02 wavd-mcs03 ]
   ```

   In this example, the load-balancing node is wavd-mcs03.

4. Exit the Cluster Resource Monitor by pressing CTRL-C on the keyboard.

B Port Bonding for Interplay MAM

Chapter Overview

The following table describes the topics covered in this chapter:

Step	Task
1	Verifying the Ethernet Ports
	Prior to configuring Port Bonding, you must first identify the ports that to be used.
2	Configuring the Ports
	Details the process for altering the existing network configuration and creating a new bonded network interface.

Port bonding (also known as link aggregation) combines multiple physical interfaces into a single logical interface. In Interplay MAM deployments, port bonding improves playback performance when multiple clients are making requests of the MCS server simultaneously. With port bonding, more concurrent playback requests can be sustained by a single server, especially for file-based playback.

Port bonding is only possible for Interplay MAM deployments. It does not apply to MediaCentral and/or Media Composer Cloud deployments.

Verifying the Ethernet Ports

In a port bonding configuration, two or more ports are grouped together. Before bonding the ports, identify the ports you wish to allocate using the RHEL setup menus.

To verify the Ethernet ports for port bonding:

1. Enter the RHEL setup menus by typing setup at the command prompt:

   ```
   setup
   ```

   The setup screen appears.

2. From the Choose a Tool menu, select the Network Configuration option and press Enter.
3. Choose the Device Configuration option and press Enter.

   A list of network interface ports appears.

4. Identify the names of the ports you plan to bond together.

   Example: eth0 & eth1

5. Exit the setup menus without making any changes by clicking Cancel and Quit.

Configuring the Ports

Port bonding requires that you modify the contents of the interface configuration file for each bonded port and create a new configuration file for the virtual bonded interface.

To configure port bonding for Interplay MAM:

1. Navigate to the directory containing the interface configuration files:

   ```
   cd /etc/sysconfig/network-scripts
   ```

2. List the directory contents to view the files:

   ```
   ls
   ```

3. Using the vi editor, open the interface configuration file for the first interface to be included in the port bond. Depending upon your server type, this could be ifcfg-eth0, ifcfg-em1, or other. In this process an HP “eth0” interface will be used as an example.

   ```
   vi ifcfg-eth0
   ```

4. When you open it for editing, the file should resemble the following example (some fields might not be present):

   ```
   DEVICE=eth0
   HWADDR=<value>
   TYPE=Ethernet
   UUID=<value>
   ONBOOT=yes
   NM_CONTROLLED=yes
   BOOTPROTO=none
   IPV6INIT=no
   USERCTL=no
   IPADDR=<value>
   NETMASK=<value>
   GATEWAY=<value>
   DHCP_HOSTNAME=$HOSTNAME
   PEERDNS=yes
   ```

   - `DEVICE=eth0`

     This specifies the name of the physical interface. This line will be different for each device. It must correspond to the name of the file itself (e.g. ifcfg-eth0).

   - `ONBOOT=yes`

     This must be set to “yes” to ensure that Linux brings up the port at boot time.

5. If present, remove the following fields from the configuration:

   - `IPADDR=<`*`value`*`>`
   - `NETMASK=<`*`value`*`>`
   - `GATEWAY=<`*`value`*`>`

6. Add port bonding configuration information for the device by inserting or altering the following lines:

   - **`MASTER=bond0`**

     This specifies the name (“bond0”) of the port bonding interface. This must be the same in each network script file in the port bonded group.

- **`SLAVE=yes`**

  This configures the interface to direct traffic through the master interface.

- **`NM_CONTROLLED=no`**

  This configures the interface to use the local file (e.g. ifcfg-eth0) for all configuration information instead of the Linux Network Manager.

7. Save and exit the vi session. Press <ESC> and type: **`:wq`**
8. Repeat the above steps for each interface to be included in the port bond group (e.g. eth1, eth2, etc.)
9. Using the Linux vi editor, create a new port bonding network script file in the same directory:

   ```
   vi ifcfg-bond0
   ```

   Where “ifcfg-bond0” is the name of the port-bonding group.
10. Add the following lines to the newly created file:

    ```
    DEVICE=bond0
    IPADDR=<value>
    NETMASK=<value>
    GATEWAY=<value>
    ONBOOT=yes
    BOOTPROTO=none
    USERCTL=no
    BONDING_OPTS=<value>
    TYPE=Ethernet
    IPV6INIT=no
    ```

    - **`DEVICE=bond0`**

      This specifies the name of the port bonding group interface. It must correspond to the name of the file itself (“ifcfg-bond0”).

    - **`BOOTPROTO=none`**

      This line indicates that the IP address of the device will be explicitly set. Alternatively, this can be configured as “BOOTPROTO=dhcp” which allows a local DHCP server to assign of the IP address device dynamically. Static addressing is the Avid recommended method for any MCS server and is a requirement for any MCS cluster deployment.

    - **`BONDING_OPTS="<value>"`**

      There are multiple ways to configure port bonding. Each is known as a “mode”. Avid supports both mode 0 and mode 4. Mode 0 (balance-rr) transmits packets in a round-robin style between the interfaces in the group. Mode 4 (802.3ad) creates an aggregation group where slave interfaces are utilized according to the 802.3ad specification.

      If you want to configure port bonding for mode 0, use the following for <*`value`*> (quotes are required):

      ```
      "mode=0"
      ```

      If you want to configure port bonding for mode 4, use the following for <*`value`*> (quotes are required):

      ```
      "mode=4 miimon=100"
      ```

Mode 4 requires a switch that supports IEEE 802.3ad Dynamic link aggregation. All interfaces must match speed and duplex settings.

- **`IPADDR and NETMASK`**

  Entries are required if you are assigning a static IP address.

- **`GATEWAY`**

  A gateway address is required if you are routing outside of your primary subnet.

11. Save and exit the vi session. Press <ESC> and type: **`:wq`**
12. Restart the network service (as root):

    ```
    /etc/init.d/network restart
    ```

Once created, the network controller designations can be verified at:

```
/etc/udev/rules.d/70-persistent-net.rules
```

The port bonding configuration can be confirmed using the following command:

```
cat /proc/net/bonding/bond0
```

C Avid iNEWS Integration

Chapter Overview

The following table describes the topics covered in this chapter:

Step	Task
1	Verifying MediaCentral Licenses on iNEWS
	A process to verify the licensing scheme on the iNEWS servers.
2	Editing SYSTEM.CLIENT.VERSIONS
	This section includes steps to add the MediaCentral UX client version to iNEWS.
3	Editing SYSTEM.CLIENT.WINDOWS
	If not using an iNEWS site licence, client IP addresses must be added to an iNEWS stroy.

Before connecting to an iNEWS newsroom computer system from a MediaCentral workstation, two iNEWS system files must be edited so that MediaCentral is recognized as a licensed device.

The files to edit are:

- SYSTEM.CLIENT.VERSIONS
- SYSTEM.CLIENT.WINDOWS

Additional files must be edited to ensure proper licensing for iNEWS integration with the MediaCentral mobile application. For more information, see "Avid MediaCentral | UX Mobile Application" on page 296.

Verifying MediaCentral Licenses on iNEWS

Before MediaCentral connects to iNEWS, verify that iNEWS is configured with the proper number of MediaCentral devices authorized to connect to the system based on the purchased licenses. iNEWS licensing limits can be identified from the iNEWS console using the following command:

```
t NRCS-A$ status license
```

A message similar to the following will appear on your screen:

```
A is ONLINE and has been CONFIGURED. ID is INWS.
System is AB. Master is A.
Disk status is OK. The database is OPEN.
Site Key............. : 009999
CPUs................. : 3
Workstation addresses : 3000
Workstation resources : 1000
COM resources........ : 5
Web Access resources. : 2
Web Client resources. : 10
Web API resources.... : 5
Wire Server resources : 8
Instinct resources... : 10
Mobile devices allowed: 2000
Community Sessions... : allowed.
```

The three lines to pay attention to are:

- Workstation addresses—indicates how many IP and/or MAC addresses can be specified in the SYSTEM.CLIENT.WINDOWS story. This story may be deleted from the iNEWS database if “Workstation addresses” shows a “site” license and IP-specific restriction is not wanted.
- Workstation resources—the number of clients that can simultaneously connect to iNEWS, including iNEWS workstations, MediaCentral workstations, Apple iPad tablets, and Apple iPhone devices.
- Mobile devices allowed—the number of mobile devices that can simultaneously connect to iNEWS.

Any time the iNEWS newsroom computer system is configured, your licensing information is checked. An error message appears in iNEWS if the configuration file defines more devices than are licensed.

Editing SYSTEM.CLIENT.VERSIONS

Some steps in the following procedure are conducted at the iNEWS console in superuser mode. For more information, see “The iNEWS Console” chapter in the *iNEWS Setup and Configuration Guide*.

For the correct iNEWS client version, see the *Avid MediaCentral Platform Services ReadMe*.

To edit the SYSTEM.CLIENT.VERSIONS story in iNEWS:

1. Sign in to an iNEWS workstation as a system administrator, or any user account with write access to the System directory.
2. Navigate to `SYSTEM.CLIENT.VERSIONS` and open the first story in that queue.

3. On a new line, add the version of the iNEWS Client module that will run on the MediaCentral server.

   To obtain the correct version of the iNEWS Client module, see the *Avid MediaCentral Platform Services ReadMe*.

4. Save the story.
5. Reconfigure the system. From the iNEWS console:
   a. Select the master computer, which is typically server A.
   b. Enter superuser mode, using the correct password.

      The dollar sign ($) at the end of the console prompt should change to a pound sign (#).

   c. Take the system offline by typing:

      ```
      NRCS-A# offline
      ```

   d. Reconfigure the system by typing:

      ```
      NRCS-A# configure -n
      ```

      The above command must be run on the master computer.

   e. When the prompt reappears, bring the system back online by typing:

      ```
      NRCS-A# online
      ```

   f. Press Ctrl+D to leave superuser mode.

      The pound sign (#) at the end of the console prompt should change back to a dollar sign ($).

Editing SYSTEM.CLIENT.WINDOWS

The following procedure only applies to sites that are not using a “site” license as Workstation addresses in iNEWS. You can review your site license information from the iNEWS console. For more information, see “Verifying MediaCentral Licenses on iNEWS” on page 274.

Some steps in the following procedure are conducted at the iNEWS console in superuser mode. For more information, see “The iNEWS Console” chapter in the *iNEWS Setup and Configuration Guide*.

To edit the SYSTEM.CLIENT.WINDOWS story in iNEWS:

1. Sign in to an iNEWS workstation as a system administrator, or any user account with write access to the System directory.
2. Navigate to `SYSTEM.CLIENT.WINDOWS` and open the first story in that queue.
3. Add the IP address of the MCS server to a new line. Use a semicolon to add helpful commentary for future reference to the end of the line.

   For instance, type:

   125.1.100.5 ;MediaCentral middleware server

   If there are multiple MCS servers, you must add the IP address for each one on individual lines in the story.

You do not need to add the IP addresses of any MediaCentral client computers or devices to the SYSTEM.CLIENT.WINDOWS story.

4. Save the story.

5. Reconfigure the system. From the iNEWS console:
   a. Select the master computer, which is typically server A.
   b. Enter superuser mode, using the correct password.

      The dollar sign ($) at the end of the console prompt should change to a pound sign (#).
   c. Take the system offline by typing:

      ```
      NRCS-A# offline
      ```
   d. Reconfigure the system by typing:

      ```
      NRCS-A# configure -n
      ```

      The above command must be run on the master computer.
   e. When the prompt reappears, bring the system back online by typing:

      ```
      NRCS-A# online
      ```
   f. Press Ctrl+D to leave superuser mode.

      The pound sign (#) at the end of the console prompt should change back to a dollar sign ($).

D Working with Sharded Mongo

Chapter Overview

This section includes the following topics that are not covered in the sharded Mongo installation and configuration process.

The following table describes the topics covered in this chapter:

Topic
Obtaining the Status of Sharded Mongo
This section includes a command for verifying the current status of the sharded Mongo configuration.
Checking for Stale Nodes
To ensure that data is being replicated to all sharded Mongo nodes, system administrators can periodically check the system for the existence of “stale nodes’.
Using the mongo-create-configuration Script
Used during the sharded Mongo configuration process, this section details additional options that can be used with the mongo-create-configuration script.
Uninstalling the Sharded Mongo Arbiter
Describes the process for removing the arbiter from the sharded Mongo configuration.
Troubleshooting Sharded Mongo
This section provides some information on how to troubleshoot sharded Mongo.
Recreating the Sharded Mongo Configuration
Information related to deleting and recreating the configuration.

Obtaining the Status of Sharded Mongo

To determine the status of the sharded Mongo configuration, administrators can run the “mongo-checker” script from any node:

`mongo-checker`

Prior versions of MCS required users to specify the “check-shard-status” command with this script as well as the -u (user) and -p (password) variables. MCS v2.9 enables users to run the mongo-checker command without these qualifiers. The “check-shard-status” command is used by default.

Single Zone Configuration

The following is an example of the command running on a three node Corosync cluster:

```
MONGOS_PORT=27018 SERVICE=iam
------------------------------------------------------------------------------
shard0
------------------------------------------------------------------------------
Hostname          |      state |   health |   priority |   votes |  isArbiter
-----------------------------------------------------------------------------
 wavd-mcs01:27100 |    PRIMARY |       up |          2 |       1 |      false
 wavd-mcs02:27100 |  SECONDARY |       up |          1 |       1 |      false
 wavd-mcs03:27100 |    ARBITER |       up |          1 |       1 |       true
-----------------------------------------------------------------------------
CONFIG
-----------------------------------------------------------------------------
Hostname          |      state |   health |   priority |   votes |  isArbiter
-----------------------------------------------------------------------------
 wavd-mcs01:28001 |    PRIMARY |       up |          2 |       1 |      false
 wavd-mcs02:28001 |  SECONDARY |       up |          2 |       1 |      false
 wavd-mcs03:28001 |  SECONDARY |       up |          2 |       1 |      false

MONGOS_PORT=27218 SERVICE=asset
-----------------------------------------------------------------------------
shard0
-----------------------------------------------------------------------------
Hostname          |      state |   health |   priority |   votes |  isArbiter
-----------------------------------------------------------------------------
 wavd-mcs01:27200 |    PRIMARY |       up |          2 |       1 |      false
 wavd-mcs02:27200 |  SECONDARY |       up |          1 |       1 |      false
 wavd-mcs03:27200 |    ARBITER |       up |          1 |       1 |       true
-----------------------------------------------------------------------------
CONFIG
-----------------------------------------------------------------------------
Hostname          |      state |   health |   priority |   votes |  isArbiter
-----------------------------------------------------------------------------
 wavd-mcs01:28201 |    PRIMARY |       up |          2 |       1 |      false
 wavd-mcs02:28201 |  SECONDARY |       up |          2 |       1 |      false
 wavd-mcs03:28201 |  SECONDARY |       up |          2 |       1 |      false
```

The output of the command provides status of the sharded Mongo configuration for both avid-iam and avid-asset. In two or three node MCS configurations, the “isArbiter” column lists the node that is acting as the sharded Mongo arbiter. In this example wavd-mcs03, a Corosync load-balancing node, is the arbiter for both avid-iam and avid-asset.

The CONFIG section lists which node is acting as the configuration server. The config service for avid-iam exists on the first seven nodes in the sharded Mongo configuration. The config service for avid-assest exists on 1 to 3 nodes per zone. In the example above, wavd-mcs01 is the primary config server for both databases. In this example, the primary config service is running on the primary shard. However, this might not always be the case.

Multi-Zone Configuration

The following is an example of the command running on a multi-zone configuration consisting of two zones:

```
MONGOS_PORT=27018 SERVICE=iam
----------------------------------------------------------------------------
shard0
----------------------------------------------------------------------------
Hostname          |      state |  health |   priority |   votes |  isArbiter
----------------------------------------------------------------------------
 wavd-mcs01:27100 |    PRIMARY |      up |          2 |       1 |      false
 wavd-mcs02:27100 |  SECONDARY |      up |          1 |       1 |      false
 wavd-nyc:27100   |  SECONDARY |      up |          0 |       1 |      false
----------------------------------------------------------------------------
shard1
----------------------------------------------------------------------------
Hostname          |      state |  health |   priority |   votes |  isArbiter
----------------------------------------------------------------------------
 wavd-nyc:27101   |    PRIMARY |      up |          2 |       1 |      false
 wavd-mcs02:27101 |  SECONDARY |      up |          0 |       0 |      false
 wavd-mcs01:27101 |  SECONDARY |      up |          0 |       0 |      false
----------------------------------------------------------------------------
CONFIG
----------------------------------------------------------------------------
Hostname          |      state |  health |   priority |   votes |  isArbiter
----------------------------------------------------------------------------
 wavd-mcs01:28001 |  SECONDARY |      up |          2 |       1 |      false
 wavd-mcs02:28001 |    PRIMARY |      up |          2 |       1 |      false
 wavd-nyc:28001   |  SECONDARY |      up |          2 |       1 |      false

MONGOS_PORT=27218 SERVICE=asset
----------------------------------------------------------------------------
shard0
----------------------------------------------------------------------------
Hostname          |      state |  health |   priority |   votes |  isArbiter
----------------------------------------------------------------------------
 wavd-mcs01:27200 |    PRIMARY |      up |          2 |       1 |      false
 wavd-mcs02:27200 |  SECONDARY |      up |          1 |       1 |      false
 wavd-nyc:29200   |    ARBITER |      up |          1 |       1 |       true
----------------------------------------------------------------------------
CONFIG
----------------------------------------------------------------------------
Hostname          |      state |  health |   priority |   votes |  isArbiter
----------------------------------------------------------------------------
 wavd-mcs01:28201 |    PRIMARY |      up |          2 |       1 |      false
 wavd-nyc:30201   |  SECONDARY |      up |          2 |       1 |      false
 wavd-mcs02:28201 |  SECONDARY |      up |          2 |       1 |      false
```

Notes for avid-iam:

In this example, Zone 1 (shard0) consists of a two-node MCS cluster running MCS v2.9. wavd-mcs01 has a priority of 2 which indicates that it is the primary node in the cluster. wavd-mcs02 has a priority of 1 indicating that it is the secondary. wavd-nyc is present as a secondary replica set member. A priority of zero indicates that it will never become a primary for that zone. wavd-nyc has a "votes" status of 1 which enables it to provide a vote for an election in the event of a fail-over.

Zone 2 (shard1) is a single-server (wavd-nyc) configuration running MCS v2.8. This node has a priority of 2 in its zone which indicates that it is the primary. Other nodes act as secondary replica set members with zero priority and votes for this zone.

Since arbiters are not required for the avid-iam database in multi-zone configurations, the "isArbiter" column lists all nodes as "false".

Notes for avid-asset:

Since Zone2 (shard1) is still running a prior version of MCS software that does not include the avid-asset service, only Zone1 reports a status for that service. Also notice that since this is a multi-zone configuration, the single server in Zone2 has been selected as the arbiter for Zone1.

For information on additional deployment types, see "MongoDB" in the *MediaCentral Platform Services Concepts and Clustering Guide*.

Additional Notes

The "state" column lists the PRIMARY and SECONDARY nodes in the configuration. However, this column might also list other conditions such as RECOVERING or DOWN. For more information on additional state conditions, refer to the following MongoDB page:

https://docs.mongodb.com/manual/reference/replica-states/

The `mongo-checker` script includes multiple variables which can be viewed through the help option:

```
mongo-checker -h
```

One of the more useful options is "`-s`" which limits the output of the script to a single service (avid-iam or avid-asset). The following example shows the usage of this command:

```
mongo-checker check-shard-status -s=iam
```

As a reminder, Mongo clustering and Corosync clustering are independent systems. The sharded Mongo primary node may not always be the Corosync master node.

Checking for Stale Nodes

A “stale” node is a member of the sharded configuration whose data has become out of sync with the data on the primary node. When a replica member becomes stale, it enters a “recovery mode” where all read operations are redirected to other replica members. This redirection away from the local node affects performance of the sharded Mongo environment. Additionally, nodes with stale replica members do not work in disconnected mode (data from remote zones is not accessible).

The same “mongo-checker” script that is used to check the status of the configuration can be used with different commands to check and fix any Mongo stale nodes. The following section provides a list of variables used with this command as well as an example output of the script:

`mongo-checker [`*`command`*`]`

Commands:

- `check-shard-status` — Reports the current status of the sharded Mongo configuration as detailed in the previous section
- `check-stale-nodes` — Detect stale replica set members
- `fix-stale-nodes` — Fixes stale replica set members
- `-h` — Shows the help options for this command

Prior versions of MCS required the -u (user) and -p (password) variables to be entered with each command. MCS v2.9 enables users to run the mongo-checker command without these variables.

The following is an example of the `check-stale-nodes` command where a stale node has been identified:

```
mongo-checker check-stale-nodes

replica member running on 27100 port is ok.
ERROR: Found stale replica's member running on 27101 port.
replica member running on 28001 port is ok.
replica member running on 27200 port is ok.
replica member running on 28201 port is ok.
```

To fix the stale node, run the mongo-checker command from any node with the “fix” option:

`mongo-checker fix-stale-nodes`

Using the mongo-create-configuration Script

The `mongo-create-configuration` script used during the sharded Mongo configuration process has multiple switch options which determine how the script is executed. One of these options is used during the sharded Mongo configuration process outlined in this guide, but other switches exist. The following information details the operation of the script and provides additional options that can be used when troubleshooting or analyzing the collected data.

The `mongo-create-configuration` script is located at `/opt/avid/bin/`, however the script can be launched from any location (no need to navigate to the /opt/avid/bin/ directory first).

If you run the `mongo-create-configuration` script more than once from the same node, a backup of the previous configuration is created. The backup includes a copy of the `hosts` file, `host_vars` folders, `group_vars` folders, and other necessary configuration files. The backup is created in case you need to revert to the previous configuration for any reason. Backup files are located at: `/opt/avid/installer/ansible/backup/<date+time-stamp>/`

Command options:

- **`mongo-create-configuration`**

  Running the script with no options collects data about the system and displays it on the screen.

  In a multi-zone configuration the script is run on the master node of the master zone. The script polls `/opt/avid/bin/avid-ics-zone-linker` and collects a list of all zones and URLs. It then connects to each URL through SSH and checks if the remote zone is a single server or a cluster. If it is a cluster, the script first gathers a list of nodes through the “crm_node -p” command. It then identifies the master, slave, and load-balancing nodes by analyzing where the ms_drbd_postgres resource is located.

- **`mongo-create-configuration -e<`*`file`*`>.csv`**

  The -e switch instructs the script to gather information about the configuration and export the information to a comma separated value file. The .csv file can be reviewed for configuration errors and corrected if necessary. No space is required between the **`-e`** and **`<`*`file`*`>`** values.

  Where <*file*> is the user designated name of the .csv file. Example usage:

  ```
  mongo-create-configuration -eWAVD.csv
  ```

- **`mongo-create-configuration -c`**

  The -c switch instructs the script to create or update the configuration files. Prior to using the -c option, Avid recommends running this command once without any options to verify that the configuration information printed to the screen is accurate.

- **`mongo-create-configuration -c<`*`file`*`>.csv`**

  Using the -c switch in combination with a file name instructs the script to update the configuration files using the contents of the specified .csv file. No space is required between the **`-c`** and **`<`*`file`*`>`** values.

  Where <*file*> is the user designated name of the .csv file. Example usage:

  ```
  mongo-create-configuration -cWAVD.csv
  ```

- **`mongo-create-configuration -d`**

  The -d switch creates a debug output that can be used for troubleshooting.

As discussed in the Sharded MongoDB chapter, when used with the -c switch, the mongo-create-configuration script creates the following files:

- `/opt/avid/installer/ansible/hosts`

  This file contains all shard names and other configuration data.

- `/opt/avid/installer/ansible/host_vars/node<#>`

  A node file containing configuration information is created for each Mongo shard.

When implementing the final sharded Mongo configuration, these files provide the source data used by the `mongo-playbook-setup` script to configure the system.

In versions of MCS prior to v2.9, Corosync load-balancing nodes were not added to the ansible hosts file. MCS v2.9 altered the sharded Mongo configuration strategy to create files for each node at `/opt/avid/installer/ansible/host_vars/` and to include all nodes in the ansible hosts file.

Whenever running the `mongo-create-configuration` script (with the `-c` option) on any MCS system running v2.6 or later with an existing sharded Mongo environment, the script polls the existing configuration as it would with a new installation. Because of this change, users might see updates to the ansible hosts file when either:

- Upgrading to MCS v2.9 or later
- Adding a new zone to a multi-zone environment

For example in an MCS v2.8 multi-zone configuration with two zones consisting of two 3-node clusters, running the script results in the following hosts file:

```
[shards]
shard0 shard_tag=region-0
shard1 shard_tag=region-1

[mcs_servers]
node0 ansible_host=wavd-mcs01
node1 ansible_host=wavd-mcs02
node2 ansible_host=nyc-01
node3 ansible_host=nyc-02
```

When upgrading this environment to MCS v2.9, the `mongo-create-configuration` script produces the following results:

```
[shards]
shard0 shard_tag=region-0
shard1 shard_tag=region-1

[mcs_servers]
node0 ansible_host=wavd-mcs01
node1 ansible_host=wavd-mcs02
node4 ansible_host=wavd-mcs03
node2 ansible_host=nyc-01
node3 ansible_host=nyc-02
node5 ansible_host=nyc-03
```

Notice that the load-balancing nodes from each zone have been added to the configuration as “node4” and “node5”. Also notice that the nodes are not *listed* numerically, but they have been **added** numerically.

If upgrading or making a configuration change, it is important to make sure that the node#’s associated with each server do not change. A change in node numbers could result in a misconfigured sharded Mongo environment and lead to service failures impacting system functionality.

Uninstalling the Sharded Mongo Arbiter

In some situations, a system administrator might need to remove the sharded Mongo arbiter that was created during the original configuration. For instance, when adding a third node to a two-node cluster, the administrator might prefer to relocate the arbiter to the load balancing node. Alternatively, sites expanding from a single-zone cluster configuration must remove the avid-iam arbiter if expanding to a multi-zone environment where arbiters are not required.

The arbiter can either be removed through a script or through a manual process. See one of the following sections to remove the arbiter:

- "Using the "remove arbiter" Script" on page 284
- "Uninstalling the Sharded Mongo Arbiter for Windows" on page 286
- "Uninstalling the Sharded Mongo Arbiter for Linux" on page 287

Using the "remove arbiter" Script

In the event that you need to remove the arbiter from the sharded Mongo configuration, Avid provides a script to assist in automating the process. The `mongo-playbook-remove-arbiter` script can be used to remove the arbiter from either a Linux or Windows system. The Linux arbiter can be either a Corosync load-balancing node or a non-Avid Linux system.

When used with a Linux system, the script completes the following tasks:

- Removes the Avid-specific services added by the sharded Mongo process
- Removes the arbiter from the sharded Mongo configuration.

The script does not remove the sharded Mongo packages from the system in case they are used by other non-Avid applications. The local /etc/hosts file on the arbiter is also not altered by the script.

When used with a Windows system, the script completes the following tasks:

- Removes the two Windows services added by the installer
- Uninstalls the MongoDB <*version*> (64 bit) application
- Deletes the c:\mongodb folder and its contents
- Removes the sharded Mongo node information from C:\Windows\System32\drivers\etc\hosts
- Removes the arbiter from the sharded Mongo configuration.

The same script is used for removing either a Linux or Windows arbiter. The script determines the arbiter's operating system and performs the appropriate actions to remove the software.

Sharded Mongo arbiters installed on a Windows system for MCS v2.6 and 2.7 followed a different configuration process. Due to the differences in the process, the "remove arbiter" script cannot be used on those systems. To remove a Windows-based arbiter that was originally configured for MCS v2.6 or v2.7, refer to "Uninstalling the Sharded Mongo Arbiter for Windows" on page 286. If you are unsure when the original arbiter was created, use the remove script as described below. If the script fails, proceed to the manual uninstall process.

To remove the sharded Mongo arbiter:

1. From the sharded Mongo management node, run the “remove-arbiter” script:

   ```
   mongo-playbook-remove-arbiter
   ```

   The sharded Mongo “management node”, is the system where the /opt/avid/installer//ansible/hosts and /opt/avid/installer//ansible/hosts_vars/node<#> files are located.

   The script is executed and completes the appropriate tasks to remove the arbiter from the configuration. The following shows an example of the final results:

   ```
   PLAY RECAP***************************************************

   Node0      : ok=6    changed=1    unreachable=0    failed=0
   Node1      : ok=3    changed=0    unreachable=0    failed=0
   Node2      : ok=11   changed=3    unreachable=0    failed=0

   COMPLETED SUCCESSFULLY
   ```

   If the script returns a “COMPLETED WITH ERRORS!!!” message, review the latest mongo-playbook-remove-arbiter_*<date>*.log file for errors at: /var/log/avid/ansible/.

2. The “remove-arbiter” script does not remove the arbiter from the /ansible/hosts file on the MediaCentral servers. This must be completed manually.

   a. On the sharded Mongo “management node”, open the following file with the Linux vi editor:

      ```
      vi /opt/avid/installer/ansible/hosts
      ```

   b. Remove the following line from the end of the configuration:

      ```
      node2 ansible_host=<arbiter_hostname>
      ```

      Where <*arbiter_hostname*> is the short host name of the arbiter.

   c. Save and exit the vi session. Press <ESC> and type: **:wq**

3. You must also manually remove the node2 information from the /ansible/host_vars directory on the MediaCentral servers.

   a. Verify the contents of the /ansible/host_vars directory:

      ```
      ls /opt/avid/installer/ansible/host_vars
      ```

      This directory should contain three folders. node0 and node1 represent the master and slave MCS servers. node2 represents the arbiter.

   b. Remove the node2 folder and its contents:

      ```
      rm -f /opt/avid/installer/ansible/host_vars/node2
      ```

4. If you are removing the arbiter from a Linux system, you must also complete the following tasks:

   - Manually remove the MediaCentral node information from the arbiter’s local /etc/hosts file.
   - If you are removing the arbiter from a Linux system that is not an MCS Corosync load-balancing node, you can also remove the sharded Mongo packages.

     ```
     yum remove mongodb-org*
     ```

     This command assumes that no other software on the system is using the MongoDB packages.
   - If you are removing the arbiter from a Linux system that is not an MCS Corosync load-balancing node, you can also remove the arbiter information from the MCS nodes’ /etc/hosts file.

5. If you are removing the arbiter from a Windows system, you must also complete the following tasks:

   - Manually remove the MediaCentral node information from the arbiter's local /etc/hosts file.
   - During the "add arbiter" process, two rules were added to the Windows firewall. If desired, these rules can be removed from the configuration. Verify that the Windows Firewall Service is running and enter the following two commands in a Windows command prompt:

     ```
     netsh advfirewall firewall delete rule name="Mongo arbiter node"
     protocol=TCP localport=27100
     ```

     ```
     netsh advfirewall firewall delete rule name="Mongo config node"
     protocol=TCP localport=28001
     ```

Uninstalling the Sharded Mongo Arbiter for Windows

If you chose not to use the Avid provided script to remove the arbiter, the process can be completed manually.

To uninstall the arbiter software on Windows:

1. Uninstall "MongoDB 3.2.4 (64 bit)" using the Windows Programs and Features Control Panel.
2. Manually remove the Mongo services:

   a. Navigate to the command prompt application: Start > All Programs > Accessories (location may vary depending on your version of Windows).

   b. Right-click on Command Prompt and select "Run as administrator".

   c. Enter the following commands to remove the services:

   ```
   sc delete mongod-iam-shard0-27100
   ```

   ```
   sc delete mongod-iam-config-28001
   ```

   ```
   sc delete mongod-asset-shard0-27200
   ```

   ```
   sc delete mongod-asset-config0-28201
   ```

   Each command should return with a "`[SC] DeleteService SUCCESS`" message.

3. The C:\mongodb folder contains old data and logs. This folder and its contents can be deleted if desired.
4. Manually remove the MCS servers that were added to the Windows hosts file at \Windows\System32\drivers\etc\hosts.
5. Remove the arbiter from the Mongo configuration by entering the following commands on either the primary or secondary Mongo node:

This process requires you to know the primary Mongo node and primary config server. The "mongo-checker check-shard-status" command can be used to verify these roles.

   a.
   ```
   mongo -u 'admin' -p 'AvidAdmin_123!' --authenticationDatabase "admin"
   <mongo_primary>:27100/admin --eval
   'rs.remove("<arbiter_hostname>:27100")'
   ```

   Where *<mongo_primary>* is the host name of the primary Mongo node and *<arbiter_hostname>* is the host name of the former Windows arbiter.

   This example assumes the default password of AvidAdmin_123!.

b.
```
mongo -u 'admin' -p 'AvidAdmin_123!' --authenticationDatabase "admin"
<primary_config_server>:28001/admin --eval
'rs.remove("<arbiter_hostname>:28001")'
```

Where *<primary_config_server>* is the host name of the primary config server and *<arbiter_hostname>* is the host name of the former Windows arbiter.

This example assumes the default password of AvidAdmin_123!.

c.
```
mongo -u 'admin' -p 'AvidAdmin_123!' --authenticationDatabase "admin"
<primary_config_server>:27200/admin --eval
'rs.remove("<arbiter_hostname>:27200")'
```

Where *<primary_config_server>* is the host name of the primary config server and *<arbiter_hostname>* is the host name of the former Windows arbiter.

This example assumes the default password of AvidAdmin_123!.

d.
```
mongo -u 'admin' -p 'AvidAdmin_123!' --authenticationDatabase "admin"
<primary_config_server>:28201/admin --eval
'rs.remove("<arbiter_hostname>:28201")'
```

Where *<primary_config_server>* is the host name of the primary config server and *<arbiter_hostname>* is the host name of the former Windows arbiter.

This example assumes the default password of AvidAdmin_123!.

If necessary, the password can be verified in the “all” file on the primary node at:

```
/opt/avid/installer/ansible/group_vars/
```

Uninstalling the Sharded Mongo Arbiter for Linux

If you chose not to use the Avid provided script to remove the arbiter, the process can be completed manually.

Throughout this process, the “mongo-checker check-shard-status” command can be used to determine the status and roles of the Mongo nodes.

To uninstall the arbiter software on Linux:

1. Prior to beginning this process, you need to determine which server is the primary Mongo node and the primary config server. Once you have identified the Mongo node roles, complete all remaining steps in this process from the primary node.

   For more information, see “Obtaining the Status of Sharded Mongo” on page 278.

2. Make a remote connection to the Mongo service on the arbiter:

   ```
   mongo <arbiter_hostname>:27100 -u 'admin' -p '<mongo_password>' --
   authenticationDatabase "admin"
   ```

   Where *<arbiter_hostname>* is the short host name of the Linux arbiter and *<mongo_password>* is the password used to connect to Mongo.

   The default password is: AvidAdmin_123!

   This command opens a Mongo command shell.

3. Enter the following command to stop the mongod-iam service on the arbiter:

   ```
   db.shutdownServer()
   ```

4. Press CTRL-C to exit the Mongo command shell.

5. Make a connection to the Mongo service on the primary:

   ```
   mongo <primary_hostname>:27100 -u 'admin' -p '<mongo_password>' --
   authenticationDatabase "admin"
   ```

   Where <*primary_hostname*> is the short host name of the primary node and <*mongo_password*> is the password used to connect to Mongo.

   This command opens a Mongo command shell.

6. Enter the following command to remove the arbiter replica set:

   ```
   rs.remove(“<arbiter_hostname>:27100”)
   ```

   Where <*arbiter_hostname*> is the host name of the Linux arbiter.

7. Press CTRL-C to exit the Mongo command shell.

8. Make a remote connection to the Mongo configuration service on the arbiter:

   ```
   mongo <arbiter_hostname>:28001 -u 'admin' -p '<mongo_password>' --
   authenticationDatabase "admin"
   ```

   Where <*arbiter_hostname*> is the host name of the Linux arbiter and <*mongo_password*> is the password used to connect to Mongo.

   This command opens a Mongo command shell.

9. Enter the following command to stop the mongod-iam-config service on the arbiter:

   ```
   db.shutdownServer()
   ```

10. Press CTRL-C to exit the Mongo command shell.

11. Make a connection to the Mongo service on the primary:

    ```
    mongo <primary_config_server>:28001 -u 'admin' -p '<mongo_password>' --
    authenticationDatabase "admin"
    ```

    Where <*primary_config_server*> is the short host name of the **primary config server** and <*mongo_password*> is the password used to connect to Mongo.

The primary config server might not be the same node as the primary Mongo node.

    This command opens a Mongo command shell.

12. Enter the following command to remove the arbiter from the configuration server:

    ```
    rs.remove("<arbiter_hostname>:28001")
    ```

    Where <*arbiter_hostname*> is the host name of the Linux arbiter.

13. Press CTRL-C to exit the Mongo command shell.

14. If the arbiter was installed on a non-MCS Linux server (not a load-balancing node) and Mongo is not used for any other purpose, Mongo can be completely removed from the system with the following command:

    ```
    yum remove mongodb-org-server-mongod mongodb-org-shell
    ```

15. Manually remove the MCS servers from the arbiter’s local hosts file at: `/etc/hosts`

16. Manually remove the arbiter from the local hosts file of the Corosync Master and Slave nodes at: `/etc/hosts`

Troubleshooting Sharded Mongo

Review the following sections for additional information on troubleshooting sharded Mongo.

Determining the Location of the Arbiter

When operating in a two-node Corosync cluster configuration, a third instance of Mongo is required to function as a tie-breaker in the event of an election. An election occurs if the primary node is down due to a network outage, power loss or other. This tie-breaking node is known as an "arbiter".

To determine the location of the arbiter, refer to the process for "Obtaining the Status of Sharded Mongo" on page 278.

Log files

If the sharded Mongo `mongo-playbook-setup` script returns a "`COMPLETED WITH ERRORS!!!`" message, review the latest `mongo-playbook-setup_<date>.log` file for errors at: `/var/log/avid/ansible/`.

The following log files might also be useful when troubleshooting the initial sharded Mongo setup and configuration:

- Contents of the `/var/log/avid/ansible/` directory. Note that this directory is not present in all versions of MCS.
- Contents of the `/var/log/mongodb/` directory
- The installation log files located in the `/var/log/` directory: `ICS_install.log` and `MediaCentral_Services_<version>_Build_<build>_Linux.log`
- Contents of the `/var/log/avid/avid-iam/` directory
- Contents of the `/var/log/avid/avid-asset/` and `/var/log/avid/avid-assetgc/` directories

Some logs contain large amounts of data which can make it difficult to find the information you need. The Linux `grep` command can be used to narrow the output of the log. For example, the following command searches the avid-iam.log for lines that contain the word "error" and prints the output to the display:

```
grep -i error /var/log/avid/avid-iam/avid-iam.log
```

The `-i` option ignores the case of the word. All versions of error, ERROR, Error, etc are included.

If working with Avid Customer Care to troubleshoot an issue related to sharded Mongo, be prepared to submit all of the logs listed above as well as the following files:

- `/opt/avid/installer/ansible/hosts`
- `/opt/avid/installer/ansible/group_vars/all`
- `/opt/avid/installer/ansible/host_vars/` (all content in this folder)
- `/etc/hosts`
- `/etc/resolv.conf`

Using the avid-ics Script

The avid-ics script provides a status for a variety of MCS services and systems, including sharded Mongo.

Usage and examples:

`avid-ics status` – Provides a status on a variety of Avid services. Additionally, services that provide support roles for Avid systems such as rabbitmq, postgres, and more are also included.

`avid-ics status sharded_mongo` – Provides a status on specific sharded Mongo services.

The following is an example of the command when run on a single server (non-multi-zone):

```
[root@wavd-doc01 ~]# avid-ics status sharded_mongo
mongod-asset-config0-28201 (pid  58836) is running...
mongod-asset-shard0-27200 (pid  57474) is running...
mongod-iam-config-28001 (pid  58179) is running...
mongod-iam-shard0-27100 (pid  56812) is running...
mongos-asset-27218 (pid  60808) is running...
mongos-iam-27018 (pid  60675) is running...
```

This command can be particularly useful for a multi-zone configuration where there might be multiple `mongod-iam-shard` services.

For more information, see “Using the avid-ics Utility Script” in the *Avid MediaCentral Platform Services Concepts and Clustering Guide*.

Using the mongo-add-arbiter-configuration Script

This script is run from the sharded Mongo “management node” (where the `/opt/avid/installer/ansible/hosts` and `/opt/avid/installer/ansible/hosts_vars/node<#>` files are located) to add an arbiter to a system consisting of only two-nodes. The usage of this script is covered in the Sharded MongoDB chapter. This section provides additional information.

To obtain more information about options that can be used with this command, use the **`-h`** switch to view the help menu:

`mongo-add-arbiter-configuration -h`

If any of the following situations occur, the script exits with an error message and no changes are made to the sharded Mongo configuration:

- The user or password cannot be verified.
- The arbiter is offline or unreachable.
- (Windows arbiter only) The user neglects to run the windows-ansible-prep.ps1 script before running the add script.

If the `mongo-add-arbiter-configuration` script has already been used to add an arbiter to the configuration, any attempt to run the script again will fail. The following message is displayed:

```
[ERROR] Number of nodes in /opt/avid/installer/ansible/hosts not 2. In this
configuration, the arbiter is not needed. Check your configuration.
```

If you need to run the script again for the same node, you must first remove the node2 information from the ansible hosts file at: `/opt/avid/installer/ansible/hosts`

Reviewing avid-iam

The avid-iam service depends on the proper configuration of sharded Mongo. Without this service, users are unable to log into MediaCentral UX. This section provides a few commands to verify that avid-iam is running and configured properly.

To check the status of the service, use the following command:

```
service avid-iam status
```

This command should result in the following: `avid-iam is running      [ OK ]`

In a cluster configuration, the avid-iam service runs on the Corosync master and slave nodes under the cluster resource “AvidIam”.

If the avid-iam service is not running, check the following:

- For MCS v2.6.x:

  ```
  cat /opt/avid/etc/avid-iam/application.properties
  ```

  Verify that the following values are correct:

  ```
  ...
  masterRegion=region-0                # must NOT be default-region
  mongo.sockets=localhost:27018        # port must NOT be 27017
  mongo.username=<...>                 # must NOT be empty
  mongo.password=<...>                 # must NOT be empty
  ...
  ```

  The `mongo.sockets` port must match the port used for the mongos service (27018), since this is the service used to connect to sharded Mongo.

- For MCS v2.7.x and later:

  ```
  cat /etc/sysconfig/avid-iam
  ```

  Verify that the following values are correct:

  ```
  export AVID_IAM_MASTER_REGION=region-0          # must NOT be empty
  export AVID_IAM_MONGO_SOCKETS=localhost:27018   # port must NOT be 27017
  export AVID_IAM_MONGO_USERNAME=<...>            # must not be empty
  export AVID_IAM_MONGO_PASSWORD=<...>            # must not be empty
  ```

  The `AVID_IAM_MONGO_SOCKETS` port must match the port used for the mongos service (27018), since this is the service used to connect to sharded Mongo.

If the values in the avid-iam configuration file are incorrect, review the contents of the sharded Mongo hosts file (`/opt/avid/installer/ansible/hosts`) and the node files (`/opt/avid/installer/ansible/host_vars`).

If the avid-iam service fails to start, verify that the mongos instance is running properly. The avid-iam service requires the mongos service for the MongoDB database connection.

Reviewing avid-asset

The avid-asset service introduced with MCS v2.9.0 uses a sharded Mongo database to store the data processed by the service. It is important to note that the Mongo database used for avid-asset is a second sharded Mongo database, distinct from the database used by avid-iam.

In MCS v2.9, the avid-asset and avid-asset-gc services are only used by the “Mixed Sequence Editing” Technology Preview. If the services fail, sites that do not have this feature enabled are unlikely to encounter any issues. Sites that have enabled this feature will be unable to combine content from different asset management systems. If the services are offline, cluster configurations will generate failures for the associated resources in the crm_mon utility.

To check the status of the avid-asset service, use the following command:

```
service avid-asset status
```

This command should result in the following: `avid-asset is running     [ OK ]`

To check the status of the avid-asset-gc service, use the following command:

```
service avid-asset-gc status
```

This command should result in the following: `avid-asset-gc is running     [ OK ]`

In a cluster configuration, the avid-asset and avid-asset-gc services run on the Corosync master and slave nodes and appear in the cluster as the “AvidAsset” and “AvidAssetGc” resources.

As with the avid-iam service, the avid-asset and avid-asset-gc services use configuration files that can be reviewed for troubleshooting purposes.

To review the avid-asset configuration file, enter the following command:

```
cat /etc/sysconfig/avid-asset
```

The following is the output from a typical single-zone configuration:

```
# Avid Asset service

# Master Region (required)
# Example: "region-0"
export AVID_ASSET_MASTER_REGION="region-0"

# MongoDB Database (required)
# Example: "mongodb://localhost/asset"
export AVID_ASSET_MONGO_URI="mongodb://asset:AvidAsset_123!@localhost:27218/
asset"

# Redis Cache (optional)
# Example: "redis://localhost/1"
export AVID_ASSET_REDIS_ENABLED=false
export AVID_ASSET_REDIS_URI=

# Log Level (one of "fatal", "error", "warn", "info", "debug", "trace")
export AVID_ASSET_LOG_LEVEL="info"

# Enable/disable integration with dependent services
export AVID_ASSET_DEPENDENCY_RESOURCE_ENABLED=false

# Feature Toggles
export AVID_ASSET_FEATURE_VERSIONS_PURGE_ENABLED=true
```

To review the avid-asset-gc configuration file, enter the following command:

`cat /etc/sysconfig/avid-asset-gc`

The following is the output from a typical single-zone configuration:

```
# Avid Asset GC

# Environment
export AVID_ASSET_GC_NODE_ENV="production"

# Master Region (required)
# Example: "region-0"
export AVID_ASSET_GC_MASTER_REGION="region-0"

# MongoDB Database of Avid Asset service (required)
# Example: "mongodb://localhost/asset"
export AVID_ASSET_GC_MONGO_URI="mongodb://
asset:AvidAsset_123!@localhost:27218/asset"

# Log Level (one of "fatal", "error", "warn", "info", "debug", "trace")
export AVID_ASSET_GC_LOG_LEVEL="info"

# Feature Toggles
export AVID_ASSET_GC_STORAGE_CLEANING_ENABLED=false

# Tasks List
export AVID_ASSET_GC_CLEANING_PURGED_ASSETS_ENABLED=true
export AVID_ASSET_GC_CLEANING_PURGED_ASSETS_VERSIONS_ENABLED=true
export AVID_ASSET_GC_PURGE_DELETED_ASSETS_ENABLED=true
export AVID_ASSET_GC_PURGEABLE_AFTER_ASSET_VERSION_ENABLED=true
```

Recreating the Sharded Mongo Configuration

If you have identified a problem with the sharded Mongo environment, and have exhausted all standard troubleshooting techniques, it is possible to recreate the sharded Mongo configuration from scratch by removing the configuration information from each node.

This is accomplished through one of two Avid provided scripts:

- `mongo-playbook-clean-all`
- `mongo-clean-local`

The `mongo-playbook-clean-all` script executes the `mongo-clean-local` script on each node, clearing the sharded Mongo configuration. If run in a multi-zone environment, all nodes are included in the clean process. Additionally, the script stops the avid-iam, avid-asset and related sharded Mongo services. If you are in a cluster configuration, the AvidIam, AvidAsset, and AvidAssetGc cluster resources are placed in an unmanaged mode which eliminates errors due to failed (stopped) services.

If you need assistance with this script, run the command with the `-h` option:

```
mongo-clean-local -h
```

Once these steps are complete, you can begin the sharded Mongo configuration process again. Proceed through the sharded Mongo configuration process that is appropriate for your environment. For more information, see the Sharded MongoDB chapter.

To clean all nodes in a cluster or multi-zone configuration:

To revert the sharded Mongo configuration to a clean state on all nodes, enter the following command on the sharded Mongo "management node" (where the `.../ansible/hosts` and `.../ansible/hosts_vars/node<#>` files are located):

```
mongo-playbook-clean-all -f
```

The `-f` option indicates that you want to perform a "full" cleanup. This instructs the script to remove the Mongo hosts file and all node files located in the `/opt/avid/installer/ansible/host_vars` directory. If you do not include the `-f` option, the files must be deleted manually.

If you run the script without the `-f` option, the ansible hosts file as well as the node files are not removed from the sharded Mongo management node. In some situations, it might be desirable to save the master configuration information on the management node.

After entering the command, the script will prompt you to verify the action:

```
=============================================================================
WARNING!!! This command will remove data related to sharded mongo!
=============================================================================
```

Type **y** to continue.

If desired, you can use the `-y` switch in the command to bypass this safety check as shown here:

```
mongo-playbook-clean-all -f -y
```

To clean a single node in a cluster or multi-zone configuration:

If you do not want to clean the sharded Mongo configuration on all nodes simultaneously, the process can be run one node at a time. The `mongo-clean-local` script can be run on any sharded Mongo node (including the sharded Mongo management node in a multi-zone configuration) using the following command:

```
mongo-clean-local -f
```

The `-f` option indicates that you want to perform a "full" cleanup. This instructs the script to remove the Mongo hosts file and all node files located in the `/opt/avid/installer/ansible/host_vars` directory. If you do not include the `-f` option, the files must be deleted manually.

The use if the -f option is really only valuable on the management node, since it is the system that maintains the sharded Mongo configuration files.

In cluster configurations, the script places the AvidIam resource in an unmanaged mode which eliminates errors due to failed (stopped) services. If running the clean-local command on a cluster, the command can be run on the nodes in any order.

To clean sharded Mongo on a single-server:

The `mongo-clean-local` script can also be run on single-server environments where sharded Mongo runs in a standalone configuration. If you receive errors regarding the UMS (user management) service when logging into MediaCentral UX or if the avid-iam service does not start, you can recreate the local sharded Mongo configuration with the following steps:

1. Clean the local configuration:

   ```
   mongo-clean-local -f
   ```

   The script asks you to confirm that you wish to complete this action. Type **y** to continue.

2. Mount the RHEL ISO on the server.

3. Run the configuration file creation script specifying the "-c" switch to instruct the script to create the configuration files:

   ```
   mongo-create-configuration -c
   ```

4. Run the final setup script:

   ```
   mongo-playbook-setup
   ```

   For more information and examples for many of these steps, reference the section for "Configuring Sharded Mongo with an MCS Load-Balancing Node" on page 132.

To clean a specific instance of sharded Mongo:

MCS v2.9 includes two sharded Mongo configurations; one for avid-iam and one for avid-asset. If you need to clean the configuration for only one of these services, the `-s` switch can be used. In the following example, the configuration for avid-asset is removed from all nodes:

```
mongo-playbook-clean-all -s=asset
```

This cleans the configuration information for avid-asset and the avid-iam service and related Mongo services are unaffected. A service can also be specified when using the `mongo-clean-local` script.

If using the -s option to limit the clean process, do not use the -f (full) option. The -f option clears the ansible hosts file and related node files.

E Avid MediaCentral | UX Mobile Application

Chapter Overview

The following table describes the topics covered in this chapter:

Step	Task
1	Before You Begin
	This is a check list of items that must be completed prior to using or installing the mobile app.
2	iNEWS Configuration for Mobile Integration
	Includes processes for configuring the iNEWS servers to enable a connection from the mobile app.
3	Installing the Mobile App on an iOS Device
	A process for installing the mobile app on iOS.
4	Installing the Mobile App on an Android Device
	A process for installing the mobile app on Android.
5	Upgrading the Mobile App
	Prior to upgrading the mobile app, it can be beneficial to create a backup of the current version of the software.

The Avid MediaCentral UX mobile app enables users operating iOS and Android devices to extend MediaCentral Platform Services workflows to the mobile platform. The app enables direct, secure access to your station's iNEWS and / or Interplay Production systems.

The Avid MediaCentral UX mobile app connects to your environment in one of two ways:

- Wi-Fi
- Carrier-specific cellular service— for example, 3G, 4G or Edge

The application automatically selects the first available connection from the list of options according to the priority shown in the list.

It is vital that the fully qualified domain names (FQDN) for all MCS servers are resolvable by the domain name server (DNS) tasked with doing so. This is particularly important when MediaCentral Platform Services servers are accessed from the MediaCentral UX mobile app. Mobile devices that cannot resolve the FQDN of the MCS server(s) experience issues connecting to the player service. Hostname resolution issues might allow mobile users to sign into MediaCentral UX, but media playback is either not possible or intermittent. While adjusting the network settings directly on a mobile device is possible, manual adjustments should not be required and are not the recommended best practice.

Before You Begin

Before using the MediaCentral UX mobile app, verify the following tasks have been completed:

- If you have a cluster configuration and intend to playback media on the mobile device, ensure that GlusterFS has been installed. This is a requirement for streaming to mobile devices.

  For details, see "Replicating the File Caches using GlusterFS" on page 127.

- Verify that the Hostname in the MediaCentral "MCPS > Player" System Settings has been configured with the system's Fully Qualified Domain Name (FQDN).

  For details, see "Player Settings" on page 102.

- Confirm that the mobile device can access the MCS server(s) through a Fully Qualified Domain Name (FQDN).

  For details, see "Validating the FQDN for External Access" on page 161.

  If this process does not return expected results, contact your local IT team to assist.

- Confirm that iNEWS is properly configured for licensed integration with the MediaCentral UX mobile app.

  For details, see "Avid iNEWS Integration" on page 273.

- Verify that Wi-Fi and/or 3G/4G streams have been enabled on your MCS system.

  For details, see "Enabling / Disabling 3G and Edge Streams" on page 86.

iNEWS Configuration for Mobile Integration

If connecting to an Avid iNEWS system, system administrators might need to adjust some iNEWS system files. Editing the files enables the iNEWS servers to recognize the MediaCentral UX mobile app as a licensed device.

Complete the following two procedures to verify iNEWS configuration:

- Editing SYSTEM.CLIENT.VERSIONS
- Editing the iNEWS Configuration File

Editing SYSTEM.CLIENT.VERSIONS

You use the iNEWS console in superuser mode, for some steps in the following procedure. For more information, see the *iNEWS Setup and Configuration Guide*.

To edit the SYSTEM.CLIENT.VERSIONS story:

1. Sign in to an iNEWS workstation as a system administrator, or any user account with write access to the System directory.
2. Navigate to SYSTEM.CLIENT.VERSIONS and open the first story in that queue.
3. Confirm that the iNEWS Client module version appears as a line in the story.

   To obtain the correct version of the iNEWS Client module, see the *Avid MediaCentral Platform Services ReadMe*.

   - If the version is correct, then close the story. The remaining steps in this process are not required.

- If the version is not correct or does not appear, continue.

4. On a new line, add the version of the MediaCentral Platform Services iNEWS client module.
5. Save the story.
6. Use the iNEWS console to reconfigure the system:
   a. Select the master computer, which is typically server “A”.
   b. Enter superuser mode, using the correct password.

      The dollar sign ($) at the end of the console’s prompt changes to a pound sign (#).
   c. Take the iNEWS system offline:

      ```
      offline
      ```
   d. Reconfigure the system to update it with the changes:

      ```
      configure
      ```
   e. When the prompt reappears, bring the system back online:

      ```
      online
      ```
   f. Press Ctrl+D to leave superuser mode.

      The pound sign (#) at the end of the console’s prompt changes back to a dollar sign ($).

Editing the iNEWS Configuration File

The configuration file (`/site/config`) lists all devices, servers, and resources configured to run on your iNEWS newsroom computer system and how they are connected. If a mobile device does not appear in the configuration file, you cannot use it with the iNEWS newsroom computer system.

The MediaCentral UX mobile app uses the same G (inws) sessions in the configuration file as other MediaCentral UX browser-based clients (Chrome, Safari) or as iNEWS workstations. You need to confirm that there are enough sessions configured to handle simultaneous connections from these types of devices available to users at your site.

You need to edit the configuration file only if there are not enough sessions.

If you need to edit the configuration file, see “The iNEWS Console” and “System Configuration” chapters in the *iNEWS Setup and Configuration Guide*. Also, some steps require use of ed, the line editor. If you do not know how to use the line editor to modify lines in the file, see “The Line Editor, ed” in the *iNEWS Setup and Configuration Guide*.

To edit the iNEWS configuration file:

1. Select all servers.

Whenever you make changes to any iNEWS site file, such as the configuration file, you must select all servers in your system at the console. Unlike database stories, site files are not automatically mirrored from one computer’s disk to another.

2. Type the following command and press Enter:

   ```
   ed /site/config
   ```

   The editor displays a numerical value indicating the file size expressed as the number of characters, including spaces and returns.

The configuration file has two major sections: the host section and the device section. For MediaCentral mobile integration, both must be edited.

3. In the host section, add a resource list entry, using the following format.

   reslist <device # or range> ; <*comments*>

   For example:

   ```
   reslist 2001:2005 ;iNEWS and IPC sessions
   ```

For dual or triple server systems, the configuration file has multiple host sections to define which server handles which devices under various circumstances. You should add resource list entries to each host section.

4. In the INWS sessions section, add a resource line for the devices, using the following format:

   inws <*device # or range*> - gnews <*device name*> ;<*comment*>

   For example:

   ```
   inws 2001:2005 - gnews -
   ```

5. Type **w** to write (save) your changes to disk.

Do not use an uppercase W in this step. Uppercase W appends the file you edit to the existing file. The resulting file might be unreadable and lead to problems with running your iNEWS system.

6. Type **q** to quit the line editor.
7. (Optional) Use the configure command to test your configuration changes, using the following syntax:

   configure /site/config <*system*> <*computer*>

   For example:

   ```
   configure /site/config ab a
   ```

   When the prompt reappears, the configuration file has been checked. If the system detects any errors, it displays appropriate “bad configuration” messages.

8. Use the iNEWS console to reconfigure the system:

   a. Select the master computer, which is typically server “A”.

   b. Enter superuser mode, using the correct password.

      The dollar sign ($) at the end of the console’s prompt changes to a pound sign (#).

   c. Take the iNEWS system offline:

      offline

   d. Reconfigure the system to update it with the changes:

      configure

   e. When the prompt reappears, bring the system back online:

      online

   f. Press Ctrl+D to leave superuser mode.

      The pound sign (#) at the end of the console’s prompt changes back to a dollar sign ($).

Installing the Mobile App on an iOS Device

The following procedure assumes licensing, setup, and configuration of the MCS, iNEWS, and / or Interplay Production servers have already been completed.

To install the mobile app on an iPad or iPhone:

1. Open iTunes to access the Apple iTunes Store.
2. Locate the Avid MediaCentral UX mobile application.
3. Select the application and tap Download.

   When the MediaCentral UX mobile application is installed on your touch-screen device, an icon representing the application appears on the home screen. You can move it elsewhere like the icons for other applications.

A direct link to the Avid MediaCentral UX app on the Apple iTunes Store is provided here (link current at time of publication):

https://itunes.apple.com/us/app/avid-mediacentral-ux/id517760700?mt=8

For additional information on the configuration and usage of the MediaCentral US mobile app, see the *Avid MediaCentral User's Guide*.

Installing the Mobile App on an Android Device

The following procedure assumes licensing, setup, and configuration of the MCS, iNEWS, and / or Interplay Production servers have already been completed.

To install the mobile app on an Android device:

1. Open the Google Play Store.
2. Search for “Avid MediaCentral”.
3. Select the application and tap Install.

A direct link to the Avid MediaCentral UX app on the Google Play Store provided here (link current at time of publication):

https://play.google.com/store/apps/details?id=com.avid.avidcentral

For additional information on the configuration and usage of the MediaCentral UX mobile app, see the *Avid MediaCentral User's Guide*.

Upgrading the Mobile App

If your iOS or Android device is configured to automatically update the MediaCentral UX app, newer versions of the software will be installed automatically as they become available.

If you have deselected the option to auto-update, you must manually upgrade the app by selecting the Update button on the app from within the Apple App Store or through Google Play on Android devices.

Both the iOS App Store and Google Play limit developers, such as Avid, to have only the most recent version of the app available for download. Prior to upgrading the MediaCentral UX app, you might want to create a backup of the current version of the app. A backup enables you to restore an earlier version of the app in the event that you are unsatisfied with the updates made in the new version.

To back up apps on iOS devices:

Visit the Apple website for detailed instructions on how to back up apps on your iOS device: https://support.apple.com/en-us/HT203977

To restore apps on iOS devices:

1. Uninstall the current version of the app from your iPhone or iPad.
2. Connect the device to a desktop PC that has iTunes installed.
3. In iTunes, click on the “Apps” link from the sidebar.

   This menu displays the apps that were on your device at the time of the last backup.
4. Select the previous version of the MediaCentral UX app from the Apps pane and drag it to the device (iPhone or iPad) section of the sidebar.
5. Sync your device with iTunes.

   The previous version of the app is reinstalled on your device.

For more information on syncing your iOS device with iTunes, see the following link on the Apple website: https://support.apple.com/en-us/HT201253

To back up and restore apps on Android devices:

Android’s built-in back up features allow users to save app data, photos, passwords and other information on your Android device. Unfortunately, the backup process does not save copies of the installed apps. There are however a number of 3rd party applications that will back up your installed applications. Search the Google Play Store for backup applications and consult the app’s documentation for installation and usage instructions.

For more information on Android’s built-in back up features, see the following Google support page: https://support.google.com/playedition/answer/2819582?hl=en

F Avid MediaCentral | UX Desktop

Chapter Overview

This appendix covers the Avid MediaCentral UX Desktop application.

The following table describes the topics covered in this chapter:

Step	Task
1	System Requirements
	Details the minimum requirements for a client to run the MediaCentral UX Desktop application.
2	Installing Adobe Flash Player
	One of the system requirements, Adobe Flash Player must be installed on the client.
3	Installing MediaCentral UX Desktop
	Includes processes for installing the application for multiple scenarios.
4	Enabling MediaCentral MOS Plug-ins
	If desired, MOS plug-ins can be enabled for iNEWS workflows.
5	Launching and Working with MediaCentral UX Desktop
	General topics covering the use of the application.
- -	Upgrading MediaCentral UX Desktop
	This section includes the process for upgrading the MediaCentral UX Desktop application.
- -	Uninstalling MediaCentral UX Desktop
	Includes processes for uninstalling the application for multiple scenarios.
- -	Troubleshooting
	Includes information on error messages resulting from a mis-configuration.

In January of 2014, Google retired the Chrome Frame plugin for Microsoft Internet Explorer which consequently retired support for MediaCentral UX on Internet Explorer. In September of 2015, version 45 of the Google Chrome browser depreciated support for Netscape Plugin Application Programming Interface (NPAPI) in favor of a newer architecture called Pepper (PPAPI). This essentially eliminates support in Chrome for software such as Java, Microsoft Silverlight and many MOS plug-ins which depend on NPAPI.

MOS (Media Object Server) is an XML based communications protocol often used with newsroom production systems such as closed-caption generators and teleprompters. MOS plug-ins create a bridge between production systems and popular newsroom management systems like Avid iNEWS, adding functionality and streamlined workflows.

MediaCentral UX Desktop is a 32 bit client application incorporating an embedded version of Chrome capable of replacing a traditional web browser as an access portal for MediaCentral UX users. This application allows clients that rely on MOS plug-ins for MediaCentral UX / iNEWS workflows to continue to operate as normal.

System Requirements

MediaCentral UX Desktop has minimal requirements and in most cases matches the requirements for a web browser.

- **Operating systems**

  For information on supported operating systems, see the Compatibility Matrix: Interplay Production and MediaCentral on the Avid Knowledge Base.

- **Flash Player**

  - Desktop v1.0 – v1.1: Adobe Flash Player v18 (NPAPI) or later
  - Desktop v1.2 and later: Adobe Flash Player v18 (PPAPI) or later

- **Network**

  The application uses the same network ports to connect to the MCS servers as a web browser. For additional network port information, see the Avid Networking Port Usage Guide on the Avid Knowledge Base.

- **Screen Resolution**

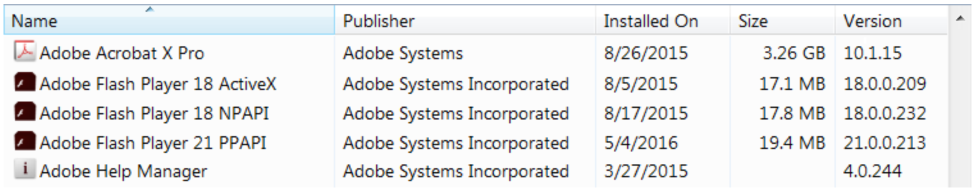
  A minimum screen resolution of 1280x1024 is required. If the size of the application window is smaller than 1280x1024, some UI elements might not be displayed.

Installing Adobe Flash Player

The client software requires Flash Player to enable playback of assets in the Media pane. Ensure that you have the correct version of Flash Player and install or update the software if necessary.

To install Adobe Flash Player:

1. (Windows only) Open the Windows Control Panel and select “Programs and Features”.
2. (Windows only) Verify your current version of Flash Player:



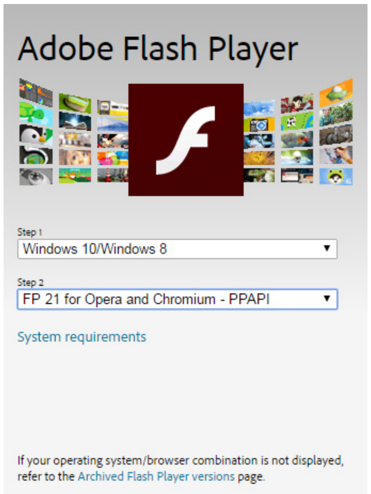
Name	Publisher	Installed On	Size	Version
Adobe Acrobat X Pro	Adobe Systems	8/26/2015	3.26 GB	10.1.15
Adobe Flash Player 18 ActiveX	Adobe Systems Incorporated	8/5/2015	17.1 MB	18.0.0.209
Adobe Flash Player 18 NPAPI	Adobe Systems Incorporated	8/17/2015	17.8 MB	18.0.0.232
Adobe Flash Player 21 PPAPI	Adobe Systems Incorporated	5/4/2016	19.4 MB	21.0.0.213
Adobe Help Manager	Adobe Systems Incorporated	3/27/2015		4.0.244

   As pictured above, multiple versions of Flash Player could be installed on your client. If you do not have the correct version installed, complete the remaining steps in this process to obtain the required software.

3. Open the web browser of your choice and navigate to:

   https://get.adobe.com/flashplayer/otherversions/

4. Select the appropriate operating system from the first pull-down menu.



Adobe Flash Player

Step 1
Windows 10/Windows 8

Step 2
FP 21 for Opera and Chromium - PPAPI

System requirements

If your operating system/browser combination is not displayed, refer to the Archived Flash Player versions page.

5. Select the version of Flash from the second pull-down menu:
   - Windows: FP <*version*> for Opera and Chromium – PPAPI
   - Mac: FP <*version*> Mac for Opera and Chromium – PPAPI

The Opera browser does not need to be installed on your client to install this version of Flash Player.

6. Click the “Download Now” button and follow the prompts to complete the installation.

   If Flash is not installed or the wrong version (NPAPI / PPAPI) is installed, the MediaCentral UX Media pane prompts the user to install Flash.

Installing MediaCentral UX Desktop

The software can be installed locally on a single client or installed remotely on multiple clients through Domain Group Policy. Review the information below and select the process that best meets your installation requirements.

- Single Client Installation
- Domain Group Deployment for Windows
- Command Line Deployment for Mac

Single Client Installation

Installing the software on a single client is accomplished through an executable installer application and a manual edit of a configuration file. The software installation and configuration requires administrator-level access to the Windows or Mac client.

Installing the Client Software for Windows

To install MediaCentral UX Desktop for Windows:

1. Sign into the Windows client as a user with administrator-level access.

2. Download MediaCentral UX Desktop from the Avid Download Center:

   http://esd.avid.com/Login.aspx
3. Unzip the installer to a new folder.
4. Launch “MediaCentral_UX_<*version*>_Win.exe” and accept the defaults to install the application.
5. Continue to “Editing the Configuration File” on page 305.

Installing the Client Software for Mac

To install MediaCentral UX Desktop for Mac:

1. Sign into the Mac client as a user with administrator-level access.
2. Download MediaCentral UX Desktop from the Avid Download Center:

   http://esd.avid.com/Login.aspx
3. Double-click on “MediaCentralUX_<*version*>.dmg” to open the disk image file.
4. Click the MediaCentral UX Installer package “MediaCentral UX Installer.pkg” to install the application.

   Accept the defaults for the installation process and enter your password when prompted.
5. Continue to “Editing the Configuration File” on page 305.

Editing the Configuration File

The client application can connect to one or more MediaCentral Platform Services (MCS) systems within your network through a local configuration file (config.txt) that defines MCS system descriptions and hosts. While there is no limit to the number of systems that can be added to the configuration file, it must contain at least one system for the application to operate.

The following table lists the content of the configuration file:

Value	Example	Value Description
Description	“WAVD Central”	This is a “friendly” name of the MCS system. This name will appear in the System menu within the user interface. The description has no character limit. It can contain spaces and other special characters. Two exceptions to this rule are the equals sign “=” and the comma “,” which have special meaning within the configuration file.
Host address	http://<*host*>	<*host*> is the FQDN of the MCS server or cluster.

To edit the configuration file:

1. Navigate to the location of the configuration file:
   - Windows: C:\ProgramData\Avid\MediaCentralUX
   - Mac: /Library/Application Support/Avid/MediaCentralUX
2. Open the config.txt file in a basic text-editing program such as Windows Notepad or Mac TextEdit.

   If a configuration file does not exist, you can manually create one.

3. Enter MCS system descriptions and hosts in the file. Each MCS system should be entered in the following format:

   ```
   description=http://<host>
   ```

   If you have multiple MCS systems, separate each with a comma.

   The following is an example of a completed configuration file with three MCS systems configured:

   ```
   WAVD Central=http://wavd-mcs,New York Office=http://192.168.45.17, London
   Office=http://lon-mcs.domain.com
   ```

4. Save and exit the file.

If an error is found in the configuration file, it can be modified to resolve the issue. Changes are immediately reflected upon the next launch of the application.

Domain Group Deployment for Windows

If your site includes multiple MediaCentral UX client systems, the software can be deployed using Windows Domain Group Policy for faster and easier installation. The process is automated through the use of a script provided by Avid with the software package. For more information on deploying software through Group Policy, see the following link:

https://support.microsoft.com/en-us/kb/816102

Configuring the Installation Script

The group deployment installation consists of two steps. The first of these steps involves editing an Avid-supplied configuration script. The second step executes the install based on script’s values.

To configure the installation script:

1. Sign into the Windows client as a user with administrator-level access.
2. Download MediaCentral UX Desktop from the Avid Download Center:

   http://esd.avid.com/Login.aspx

3. Unzip the installer to a new folder.
4. Open the “InstallMediaCentral.cmd” file in a basic text-editing program such as Notepad.
5. The script contains the following line which includes two values that require editing:

   ```
   %ScriptDIR%\MediaCentral_UX_<version>_Win.exe /s /v"/qb
   SERVERLIST="""MCSERVER=http://news-mcs""""
   ```

Value	Value Description
MCSERVER	This is a “friendly” name of the MCS system. This name will appear in the System menu within the user interface. The description has no character limit. It can contain spaces and other special characters. Two exceptions to this rule are the equals sign “=” and the comma “,” which have special meaning within the configuration file.
news-mcs	This value represents the FQDN of the MCS server or cluster.

6. Once the changes are complete, save and exit the text editor.

Running the Installation Script

The installation script can be run directly from a folder in Windows Explorer or from a command line tool such as cmd.exe. If the installation fails for any reason, the command window reports the reason for the failure which could be missed if running the script directly from a folder.

The script performs the following actions:

- Silently runs the installer (no user prompts)
- Creates the config.txt configuration file using the values defined in the script
- Copies the configuration file to “C:\ProgramData\Avid\MediaCentralUX” on the client system.

If an error is found in the configuration file, it can be modified to resolve the issue. Changes are immediately reflected upon the next launch of the application.

To Install from Windows Explorer:

1. Navigate to the folder containing the “MediaCentral_UX_<*version*>_Win.exe” installer and edited script file.
2. Double-click the “InstallMediaCentral.cmd” script to begin the installation.

   A command window appears, followed by the silent installer for the application. Once the installation is complete, the command window closes.

To Install from Command Line:

1. Use Windows Explorer to navigate to the location of the Windows command prompt software, cmd.exe:

   C:\Windows\System32
2. Right-click on cmd.exe and select “Run as administrator”.

   This ensures you have the correct level of access to install the application.
3. Use Windows Explorer to navigate to the location of the edited script file.
4. Drag the “InstallMediaCentral.cmd” installer script from the Windows folder to the command window.

   This will copy the correct path and filename to the command prompt.
5. Press Enter in the command window to begin the installation.

   The application silent installer appears and automatically closes when complete.

   A successful installation should return the following text in the command window:

   ```
   ScriptDIR= C:\Avid_Installers\

   Returncode was 0

   Install complete.
   ```

If errors occurred during the installation, the Returncode identifies the source of the issue.

6. Once the installation is complete, close the command window.

Command Line Deployment for Mac

Unlike the Windows installer, the MediaCentral UX Desktop installer for Mac does not include an installer script. However, the application can be installed through command line for faster deployment on multiple systems.

To install from command line:

1. Create a folder on a network share that can be accessed by all Mac clients.
2. Copy the MediaCentral UX Desktop installer to the folder on the network share.
3. Open the disk image file (MediaCentralUX_<*version*>.dmg) and extract the “MediaCentral UX Installer.pkg” file by dragging the .pkg icon to the folder.
4. Create a custom config.txt file for your environment and place the file in the same folder as the .pkg file.

   For details on creating the config.txt file, see “Editing the Configuration File” on page 305.
5. Mount the network share on each Mac client.
6. Open the Terminal application (Mac HD/Applications/Utilities/Terminal) on the client and enter the following command:

   ```
   sudo installer -pkg <installer path> -target <target path>
   ```

   Where the following values are used:

   - <*installer path*> is the path and filename of the installer application.
   - <*target path*> is location where you intend to install the application on the local system. A forward slash in the target variable “-target /” can be used to specify the local boot drive.

   The following is an example of the command:

   ```
   sudo installer -pkg /Volumes/Engineering/Installer/MediaCentral\ UX\
   Installer.pkg -target /
   ```
7. You may receive a warning regarding improper use of the sudo command.

   Enter your user password to continue. Text similar to the following appears:

   ```
   installer: Package name is Avid MediaCentral UX

   installer: Installing at base path /

   installer: The install was successful.
   ```

   The application is installed to the specified location and the config.txt file is copied to the /Library/Application Support/Avid/MediaCentralUX on the local client.

Enabling MediaCentral MOS Plug-ins

MediaCentral provides support for MOS Active-X plug-ins. For example, Deko Select is a plug-in for a newsroom computer system’s interface that allows a user, such as a reporter, to drag and drop graphic templates directly into the story, as well as alter replaceable text or graphics in the selected template. Other plug-ins are available through third-party manufacturers.

These plug-ins are specific to iNEWS workflows. They are available in Rundown, Story, Log and Cut layouts. MOS Plug-ins are only available for clients on the Windows operating system.

Installing Plug-Ins

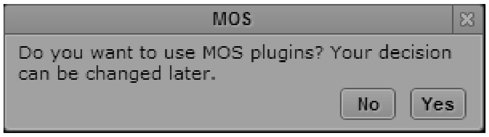
MediaCentral UX Desktop includes the supporting infrastructure needed for Active X controls, but not the plug-ins themselves. Users need to install the individual MOS plug-ins required for their workflow. For procedures on how to install plug-ins, see the documentation for the plug-in.

After installation and configuration, plug-ins are listed at the bottom of the Panes menu.

Users that have been using MOS plug-ins with MediaCentral UX in a web browser do not need to reinstall the plug-ins.

Enabling MOS

When a newly created user first signs in to MediaCentral UX Desktop, the user is prompted with the following message:



MOS

Do you want to use MOS plugins? Your decision can be changed later.

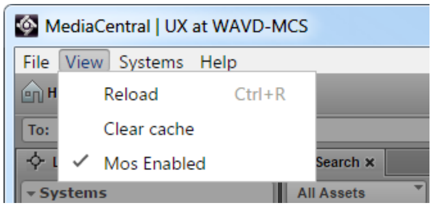
Selecting Yes or No will appropriately enable or disable the use of any MOS plug-ins installed on the workstation. If the user selects “No”, but later wants to use MOS plug-ins, the feature needs to be enabled.

MediaCentral UX includes a setting to enable or disable MOS integration. In MediaCentral UX Desktop v1.0 - v1.1, this setting is located in the MediaCentral UX User Settings window. In MediaCentral UX Desktop v1.2 and later, the MOS settings are enabled through the Desktop View menu.

After changing the setting to enable or disable MOS capabilities, the user must sign out and sign back in to MediaCentral UX for the changes to take effect.

To enable MOS plug-ins with Desktop v1.2 and later:

1. Sign into MediaCentral UX as the user that requires access to MOS plug-ins.
2. Select the View menu from the MediaCentral UX Desktop interface.

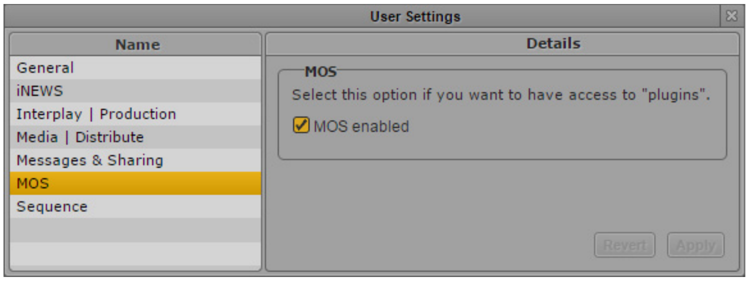


3. Select the option for “Mos Enabled”.
4. Sign out of MediaCentral UX and relaunch the Desktop application to enable the change.

To enable MOS plug-ins with Desktop v1.1 and earlier:

1. Sign into MediaCentral UX as the user that requires access to MOS plug-ins.

2. Select Home > User Settings > MOS



MOS

Select this option if you want to have access to "plugins".

☑ MOS enabled

3. Select the check box for “MOS enabled.”
4. Click Apply.
5. Sign out of MediaCentral UX and relaunch the Desktop application to enable the change.

Launching and Working with MediaCentral UX Desktop

The desktop application maintains the same feature set as the MediaCentral UX web browser experience. However, the methods used to access the MCS servers are slightly different. This section includes the following topics:

- Launching the Application
- Working with the Menu System on Windows
- Working with the Menu System on Mac
- Accessing Additional MCS Systems
- Selecting a Deep Link

Launching the Application

Once installed, the application can be found and launched from the following locations:

- **Windows 7**: Through the shortcut added to the Desktop or through the Start menu at All Programs > Avid > MediaCentral UX.
- **Windows 8**: Through the tile added to the Windows 8 Start Screen or through the shortcut added to the Desktop.
- **Windows 10**: Through the shortcut added to the Desktop or through the Start menu at All apps > Avid > MediaCentral UX.
- **Mac**: The application is located at: Mac HD/Applications/Avid/MediaCentralUX

  For ease of access on Mac systems, you might want to drag the application icon to the Dock.

After launching the software, sign in to MediaCentral UX as you would in a web browser.

Working with the Menu System on Windows

The Windows operating system menus include the following features:

File

- Close – Closes the application. If you have unsaved work, you will be asked if you want to save your progress before exiting.

View

- Reload – Equivalent to a refresh of a web browser. If you have unsaved work, the system asks you to verify that you want to reload the interface.
- Clear cache – Equivalent to clearing the cache in a web browser. If you believe you are seeing incorrect or stale data, clearing the cache and reloading the window should refresh the data.
- Mos Enabled – Added in Desktop v1.2, this is a user setting that can enabled or disabled to allow use of MOS plug-ins installed on the user's workstation (personal computer) within MediaCentral UX Desktop.

Systems

- Lists other MCS systems within the organization.

  For details on this feature, see "Accessing Additional MCS Systems" on page 312.

Help

- About – Provides the version of MediaCentral UX Desktop. Click anywhere outside of the About window to continue working.
- Logging – MediaCentral UX Desktop v1.3 introduced this menu option that can be enabled or disabled as desired. Logs are created on the local desktop system which can used to assist with troubleshooting issues directly related to the Desktop app. A check mark next to the option indicates that the feature is enabled

  Logs are created in: C:\Users\<*user*>\AppData\Roaming\MediaCentralUX\logs

  When enabled, up to 100 logs are created on the system. Once 100 log files have been generated, older logs are cycled (deleted) to accommodate newer logs. The maximum size of each log file is 1MB.

Working with the Menu System on Mac

The Mac operating system menus include the following features:

MediaCentralUX

- About MediaCentralUX – Provides the version of MediaCentral UX Desktop. Click anywhere outside of the About window to continue working.
- Logging – MediaCentral UX Desktop v1.3 introduced this menu option that can be enabled or disabled as desired. Logs are created on the local desktop system which can used to assist with troubleshooting issues directly related to the Desktop app. A check mark next to the option indicates that the feature is enabled.

  Logs are created in: ~/Library/Application Support/MediaCentralUX/logs

When enabled, up to 100 logs are created on the system. Once 100 log files have been generated, older logs are cycled (deleted) to accommodate newer logs. The maximum size of each log file is 1MB.

- Quit – Closes (quits) the application.

View

- Reload – Equivalent to a refresh of a web browser. If you have unsaved work, the system asks you to verify that you want to reload the interface.
- Clear cache – Equivalent to clearing the cache in a web browser. If you believe you are seeing incorrect or stale data, clearing the cache and reloading the window should refresh the data.

Systems

- Lists other MCS systems within the organization.

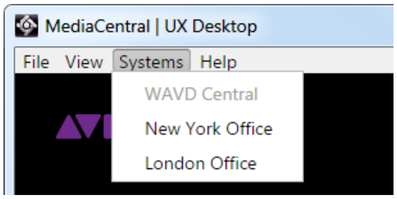
  For details on this feature, see "Accessing Additional MCS Systems" on page 312.

Window

- Close – Closes the currently active window. If you only have one window open, this essentially quits the application.
- (Sessions) If more than one MediaCentral UX Desktop window is opened, the Window menu lists each session.

Accessing Additional MCS Systems

Modern web browsers enable users to open multiple tabs, with each tab functioning as an independent browser. MediaCentral UX Desktop replicates the functionality of multiple tabs through the Systems menu. This menu is populated with one or more MCS systems by the config.txt configuration file created during the installation process.



Selecting one of the systems in this menu will open an additional MediaCentral UX Desktop window, allowing the user to sign in and work with the assets of the other MCS system.

The user needs valid user credentials on the additional MCS system to allow sign in.

Selecting a Deep Link

A *deep link* is a link to an asset on a remote MCS system that has been sent to a user through the Messaging pane. Similar to the process for accessing additional MCS systems, selecting a deep link opens an additional MediaCentral UX Desktop window.

The user needs valid user credentials on the additional MCS system to allow sign in.

Upgrading MediaCentral UX Desktop

The upgrade process for the client is similar to the installation process. Simply, launch the installer application. The previous version of the application will be uninstalled and replaced with the new version. The existing config.txt file is unaltered by the upgrade process.

Uninstalling MediaCentral UX Desktop

The client software can be removed through a few simple steps. However, the config.txt configuration file is intentionally excluded from this process. Leaving the configuration file in place enables administrators to upgrade to a new version of the application, without needing to reconfigure the settings.

To Uninstall MediaCentral UX Desktop on Windows:

1. Sign into the Windows system as a user with administrator-level access.
2. Open the Windows Control Panel and select “Programs and Features”.
3. Right-click on Avid MediaCentral | UX and select Uninstall.

   This uninstalls the software from your system, but leaves the configuration file intact.
4. (Optional) If you want to remove all traces of the application, navigate to C:\ProgramData\Avid\ and delete the MediaCentralUX folder which contains the configuration file.

To Uninstall MediaCentral UX Desktop on Mac:

1. Sign into the Mac system as a user with administrator-level access.
2. Navigate to: Mac HD/Applications/Avid_Uninstallers/
3. Launch the MediaCentral UX Uninstaller application.

   The uninstaller builds a list of files to uninstall.
4. Select the appropriate check boxes (all by default) and click the Uninstall button.
5. To assist in the removal of the software, a “helper” application is temporarily installed.

   Enter your password and click “Install Helper”.

   The “helper” application is automatically removed at the end of the uninstall process.
6. When the process has completed, click the Quit button to exit the application.

Troubleshooting

The following section describes situations that a user may encounter while working with MediaCentral UX Desktop.

Error Messages:

The following error messages could be encountered when working with the MediaCentral UX Desktop application:

- "Error connecting to the MediaCentral server. Please contact your administrator."

  This error appears in the MediaCentral UX Desktop interface if any of the following are true:

  - The configuration file is missing.
  - The configuration file exists, but is empty.
  - The selected MCS system is offline or unavailable.

  Resolution: Create or edit the config.txt file if it is missing or empty. If the configuration file is correct, ensure the MCS system you are connecting to is available.

- A JavaScript error occurred in the main process. Uncaught Exception: Cannot read property 'indexOf' of undefined"

  This error appears after launching MediaCentral UX Desktop and relates to an error in the configuration file.

  Resolution: Edit the config.txt file. Verify that commas are only used to separate MCS systems and not used anywhere else in the file (e.g. description value).

- A JavaScript error occurred in the main process. Uncaught Exception: Cannot read property 'split' of undefined"

  This error appears after launching MediaCentral UX Desktop and relates to an error in the configuration file.

  Resolution: Edit the config.txt file. Verify that equals signs (=) are only used between the description value and the host address value and not used anywhere else in the file.

Clearing the Local Cache

If you believe you are seeing stale data or there is an issue with the user interface, clearing the local cache files from the client could resolve the issue.

Users should save all work prior to completing this process.

1. Select the View menu and select "Clear cache".

   This action will sign the user out of the application.

2. Sign back into MediaCentral UX.

   Cache files are stored at: C:\Users\user\AppData\Roaming\MediaCentralUX

G MOS Active-X Plug-Ins

Chapter Overview

This section includes legacy information for enabling MOS Active-X Plug-Ins in:

- Chrome (v44 or earlier)
- Internet Explorer (legacy)

The following table describes the topics covered in this chapter:

Topics
Enabling MOS Plug-Ins in Google Chrome
This section covers the steps required to enable MOS plug-ins in legacy versions of Google Chrome.
Enabling MOS Plug-Ins in Internet Explorer
This section covers the steps required to enable MOS plug-ins in Internet Explorer 9.

The following limitations apply to enabling MOS plug-ins in a web browser:

- Chrome v45 depreciated support for the code that enables MOS plug-ins. For workflows that need to continue using MOS plug-ins, see "Avid MediaCentral | UX Desktop" on page 302.
- As of MediaCentral Platform Services v2.3, Internet Explorer is no longer a supported browser. This applies to all versions of Internet Explorer.
- Active X plug-ins are not supported in the Safari browser.

Enabling MOS Plug-Ins in Google Chrome

MediaCentral provides support for MOS Active-X plug-ins. For example, Deko Select is a plug-in for a newsroom computer system's interface that allows a user, such as a reporter, to drag and drop graphic templates directly into the story, as well as alter replaceable text or graphics in the selected template. Other plug-ins are available through third-party manufacturers.

These plug-ins are specific to iNEWS workflows. They are available in Rundown, Story, Log and Cut layouts.

The MCS installation program installs only the container needed for Active X controls. You need to install additional software as described in the following sections.

Setting Up Your Browser

The Chrome browser requires an extension that lets you use MOS plug-ins. The first time you sign in to MediaCentral, a dialog box asks if you want to use MOS plug-ins.

- If you click yes, an installer is downloaded from the MediaCentral Services server. Allow pop-ups from the MediaCentral Services server if you are informed that a pop-up was blocked, and then refresh the page. Double-click the .exe file to install the program.

  After installation is complete, close Chrome and then reopen it for the extension to be accessible by MediaCentral. Recent Chrome versions disable third-party plug-ins. Make sure that Chrome Tools > Extensions displays Enabled next to the Avid ActiveX extension.

- If you click no, and later want to use plug-ins, enable MOS as described below. The next time you sign in or refresh the application, a blank window opens and the installer is downloaded. Click the .exe file to install the extension.

  For additional information regarding support of Active-X plugins in Chrome, see the *Avid MediaCentral Platform Services v2.3 ReadMe*.

Enabling MOS

To use the plug-ins for a user you need to enable MOS in MediaCentral. Select Home > User Settings > MOS and then select "MOS enabled."

This feature is no longer available in MCS v2.5 on Chrome v45 or later.

Installing Plug-Ins

For procedures on how to install plug-ins, see the documentation for the plug-in.

After installation and configuration, plug-ins are listed at the bottom of the Panes menu.

If you do not see the plugin, review the following information on the Avid Knowledge Base:

http://avid.force.com/pkb/articles/en_US/troubleshooting/Avid-Interplay-Central-Avid-MOS-Plugin-is-disabled-by-Chrome

Uninstalling the Chrome Extension

If you need to uninstall the Chrome Extension, use the Windows Control Panel. **Do not use the Chrome Extensions page**.

1. Click Start and select Control Panel.
2. Click Programs and Features.
3. Right-click Avid MediaCentral MOS plugin and select Uninstall. Click Yes and follow the prompts.

For more information about MOS plug-ins, see the *Avid MediaCentral User's Guide* or the Avid MediaCentral UX Help.

Enabling MOS Plug-Ins in Internet Explorer

The instructions in this appendix were created using Internet Explorer 9.0.8112.16421 and Google Chrome Frame 65.169.107 on Windows 7 x86_64 SP1. Updates to any of these applications could change the steps below, including the order in which the steps are performed.

Once you complete the procedure, the Avid ActiveX container is available in IE9. When a MOS-enabled user logs in, a list of their installed ActiveX plug-ins appears at the bottom of the Panes menu. Opening a plug-in creates a new tab. (Press F5 if the tab is empty when loaded.) The tab can be dragged out of Internet Explorer, permitting drag and drop into MediaCentral UX.

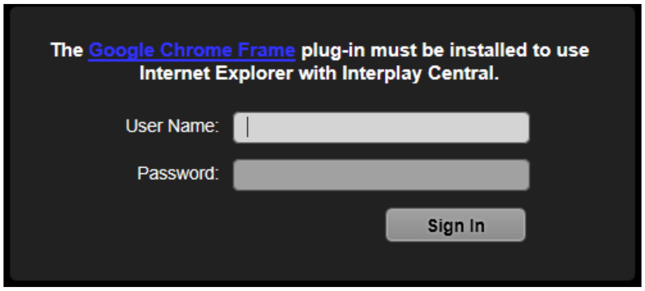
To enable MOS plug-ins in Internet Explorer:

1. Launch Internet Explorer and enter the URL of the MCS server (or cluster) in the address bar (e.g. https://<*FQDN*>).

   Where <*FQDN*> is the fully qualified domain name of the MCS server or cluster.

   Bypass the certificate warning, if one is present.

   The MediaCentral UX sign-in page informs you that the Google Chrome Frame is required.



The Google Chrome Frame plug-in must be installed to use Internet Explorer with Interplay Central.

2. Install Google Chrome Frame using the link on the sign in page.

Google Chrome Frame must be installed as user with Administrator rights. The Avid ActiveX container also requires administrator elevation.

3. A dialog should appear indicating the ChromeFrame BHO add-on from Google Inc is ready for use. Select Enable in that dialog.

4. Navigate once again to MCS server or cluster (e.g. https://<*FQDN*>) and sign in as a user for whom MOS plug-ins are enabled.

To enable MOS for the logged in user, in MediaCentral UX, select Home > User Settings > MOS and then select "MOS enabled".

5. Download and run "setup.exe" as prompted.

   If you receive a "This webpage is not available" message, refresh with F5, and then click Yes to proceed.

   Follow the instructions appearing in the Avid MediaCentral MOS plugin installation wizard, and accept the defaults to install the extension.

6. Close and re-open Internet Explorer. Navigate to MediaCentral UX and sign in as the same user. Do not download "setup.exe" again. Sign out of MediaCentral UX and close IE.

   This step forces Chrome Frame to register the Avid extension.

7. In Windows Explorer, navigate to the following directory:

   C:\Users\<*username*>\AppData\Local\Google\Chrome Frame\User Data\iexplorer\Default

8. Open the "Preferences" file in Notepad.

   For a complete example of this file, see "Sample ActiveX Object in the Preferences File" on page 319.

9. Locate the `known_disabled` key and delete the line:

   ```
   "known_disabled": [ "lmcebpepkojaapaoliodbjagahkpedph" ],
   ```

10. Search for the term "ActiveX" to find the "Avid MOS ActiveX Chrome Extension" object, and modify the "state" value from 0 to 1.

    ```
    "state": 1,
    ```

11. Save and close the Preferences file.

12. Once again, launch Internet Explorer and navigate to the MCS server or cluster (e.g. https://<*FQDN*>).

13. Sign in as the user for whom MOS plug-ins are enabled.

    Installed ActiveX plug-ins are now visible in MediaCentral UX through the Panes menu.

Sample ActiveX Object in the Preferences File

The process for Enabling MOS Plug-Ins in Internet Explorer references the Internet Explorer preference file. For reference, an example of the final ActiveX object is included below. Some values could be different for your installation.

```
         "lmcebpepkojaapaoliodbjagahkpedph": {
            "ack_prompt_count": 1,
            "active_permissions": {
               "api": [ "plugin" ]
            },
            "creation_flags": 1,
            "from_bookmark": false,
            "from_webstore": false,
            "initial_keybindings_set": true,
            "install_time": "13029963342661257",
            "location": 3,
            "manifest": {
               "description": "Avid MOS ActiveX Chrome Extension",
               "key":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCa6DtGBLy26p0nWU7mfBTutgDZpGZw0ta30LRo1
Av6J1LUgL3AxJu5BP4TJxlXXbIKd0H2X6oLgKU3GIw5+r1YKK8BKVfgjpSanEWzgvWsbjXcnH4XVF8
thXYvutkTj5telkhFmOba1UG0zauqMqpnWus9ADGyMGBUIPsTlLhXDwIDAQAB",
               "manifest_version": 2,
               "name": "Avid MOS ActiveX hosting plugin",
               "plugins": [ {
                  "path": "npchmos.dll",
                  "public": true
               } ],
               "version": "1.0.1.10"
            },
            "path": "lmcebpepkojaapaoliodbjagahkpedph\\1.0.1.10_0",
            "state": 1,
            "was_installed_by_default": false
         },
```

Avid
75 Network Drive
Burlington, MA 01803-2756 USA

Technical Support (USA)
Visit the Online Support Center
at www.avid.com/support

Product Information
For company and product information, visit us on the web at www.avid.com