MediaCentral® Platform Services

Installation and Configuration Guide Version 2.7

Important Information

This document provides instructions to install and configure Avid MediaCentral Platform Services (MCS) v2.7.

The following documents available from the MediaCentral Platform Services page of the Avid Knowledge Base are referenced in this guide:

- *Avid MediaCentral Platform Services ReadMe* – Read prior to completing any MCS installation or upgrade.
- *Avid MediaCentral Platform Services Upgrade Guide* – Reference if you are upgrading to MCS v2.7 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

***Note**: Throughout this document, "Avid MediaCentral Platform Services" is referred to as "MCS". "Red Hat Enterprise Linux" is referred to as "RHEL".*

***Note**: 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.*

***Note:** 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.*

Revision History

Date Revised	Changes Made
January 10, 2017	• Updated examples for the Customizable Logger cluster installation process.
October 17, 2016	• Minor change to the description of a step in the sharded Mongo arbiter configuration process. Informational only, no technical change.

Date Revised	Changes Made
October 3, 2106	• Added process for **Configuring Access for External Systems** on page 78. • Added upgrade related to the MAM Connector.
September 1, 2016	• Updated processes to upgrade and downgrade the Avid shared storage client.
July 22, 2016	• Step 4 of the multi-zone, slave zone registration process has been updated to indicate usage of the master zone's password.
July 21, 2016	• Added step to verify the Cluster pingable IP in the sharded Mongo configuration. • Updated information regarding the **Interplay MAM User** on page 23.
June 23, 2016	• New chapter: **PART IX: INSTALLING CUSTOMIZABLE LOGGER** • Technology Preview of the Asset Watermarking feature. For details, see **Enabling Asset Watermarking** on page 105. • Added **Using the MediaCentral Health Check Script** on page 225. • Introduction of MediaCentral Desktop v1.2. For details, see **Appendix E: Avid MediaCentral | UX Desktop** on page 261. • Added a prerequisite for the sharded Mongo arbiter. For details, see **Planning for the Mongo Arbiter** on page 16. • Added process to enable a list of trusted servers for MAM remote playback workflow. For details, see **Enabling Remote Playback** on page 117. • Updated procedure for removing a Mongo arbiter.

Contents

PART I: INSTALLATION PREREQUISITES

Chapter Overview

The purpose of this chapter is to guide the preparation of all materials needed for the MCS installation and to pre-configure 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	**Updating MediaCentral UX Licenses**	15 min
	Licensing requirements for Interplay Production and iNEWS.	
7	**Creating User Accounts**	10 min
	Convers the creation of user accounts required by MCS.	
8	**Adjusting Interplay Production Settings**	5 min
	Information on adjusting settings required by MCS.	
9	**Adding the MediaCentral UX Version to Avid iNEWS**	5 min
	Enables MediaCentral UX user to connect to iNEWS.	
10	**Installing the MediaCentral Distribution Service**	10 min
	Required for certain Interplay Production workflows.	
11	**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: IP addresses, hostnames, domain name, DNS, NTP, SNMP, etc.
- ☐ Cluster-specific information: Additional IP addresses, e-mail address
- ☐ Users: Identifying 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 | 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 MediaCentral Services page of the Avid Knowledge Base. Completing the Pre-Flight information will 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, configure **Part I** through **Part III** concurrently on all cluster nodes. **Part IV** of this installation document must be completed on the Master node only, unless otherwise instructed.

Network Interface Cards and Network Connections

Avid supports the onboard 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.

The HP DL360p Gen8 supports additional 1 Gb network adapters. See **HP DL360p Gen8 Card Placement** in Appendix A for more information.

For more information on determining 1 Gb or 10 Gb connections as well as information on supported adapters, see the *MediaCentral Platform Services Hardware Guide* located on the MediaCentral Platform Services page of the Avid Knowledge Base.

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

- ☐ Zone 1: Connected to ISIS VLAN(s) 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 to ISIS VLAN(s) 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 ISIS (one hop) and (if applicable) load-balanced across ISIS VLANs (approximately a 60/40 ratio).

  Note: *All MCS 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 ISIS and streams images and sound to the clients. This workflow requires MCS to connect to an Avid ISIS 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-ISIS storage, the network connection is at the user's discretion as long as it is a 1 Gb connection or better.

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

Avid iNEWS

iNEWS-only deployments do not require an ISIS connection. 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 failover. 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 **PART VI: SHARDED MONGO** on page 133 as well as the "MongoDB" section of the *MediaCentral Platform Services Concepts and Clustering Guide*.

***Note**: 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.

> **Note**: *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.

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 a Windows system and a SFTP tool such as WinSCP
- ☐ 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.

See **Copying Software to the MCS Server** in Appendix A for details on each of these methods.

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 plugin
  - (if applicable) Media Distribute
- ☐ GlusterFS
- ☐ (if applicable) Storage Controller Driver ISO 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.

> ***Note:*** *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).*
>
> ***Important****: 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* located on the MediaCentral Platform Services page of the Avid Knowledge Base.

MCS Installation Packages

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

> ***Note**: 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 plugin**

  The Media Composer Cloud software is a plugin 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.

***Note**: 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 higher 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” web page:

http://h17007.www1.hp.com/us/en/enterprise/servers/supportmatrix/exceptions/rhel_exceptions.aspx

***Note**: 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” web 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.

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.

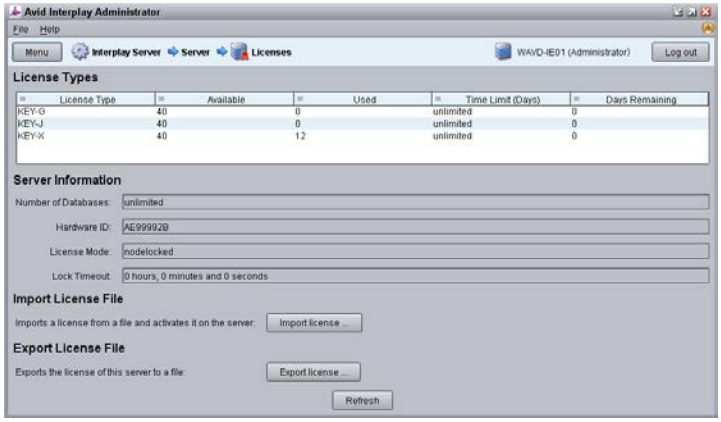
Interplay Production Licensing

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.

> ***Note**: 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. Log in using Interplay Production’s Administrator credentials.
3. From the main menu, select Server > Licenses.



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 *Interplay | 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 **Appendix C: Configuring iNEWS for Integration with MediaCentral**.

Creating User Accounts

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

- ☐ Interplay Production
- ☐ Avid ISIS
- ☐ iNEWS
- ☐ Interplay MAM
- ☐ Media Composer Cloud

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 ISIS system.

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

1. Launch the Interplay Administrator on the Interplay Engine. This can be found at: Start > Avid > Avid Interplay Access Utilities > Avid Interplay Administrator.
2. Log 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***.**

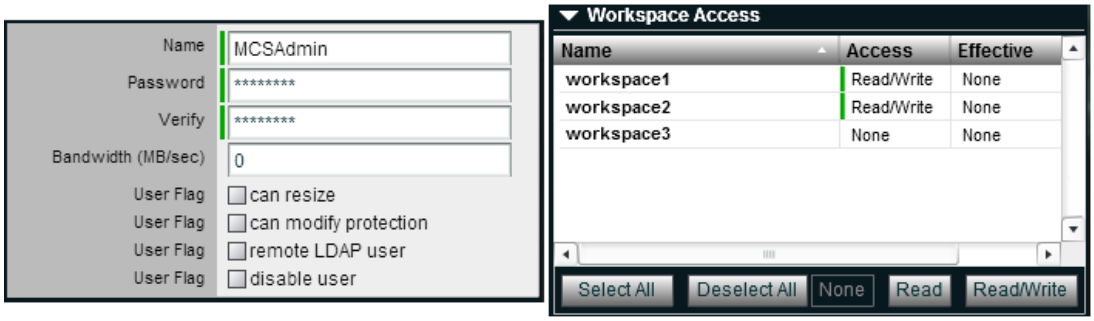
Avid ISIS User

When integrating with Interplay Production, MediaCentral UX requires credentials to access the media on the ISIS 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**

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

   ***Note**: In a failover configuration, use the virtual System Director hostname. Alternatively, the IP address of the System Director (or virtual System Director) can also be used.*
2. Log in using the ISIS 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.



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 ISIS Management Console.

   ***Note**: If you are connecting to multiple ISIS systems, ensure the same user/password is created on each ISIS.*

For additional information on users creation in Interplay Production, see the *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 115.

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 configuring the MAM Connector System Settings, see **Configuring the MAM Connector** on page 192.

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 and Platform Services Settings” or “Application Database Settings” in v3.5 and lower) 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 log into Interplay Production and Avid ISIS.
- ☐ 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 ISIS user.
- ☐ Remember that MCS runs on Linux. Both passwords **and user accounts** are case sensitive.

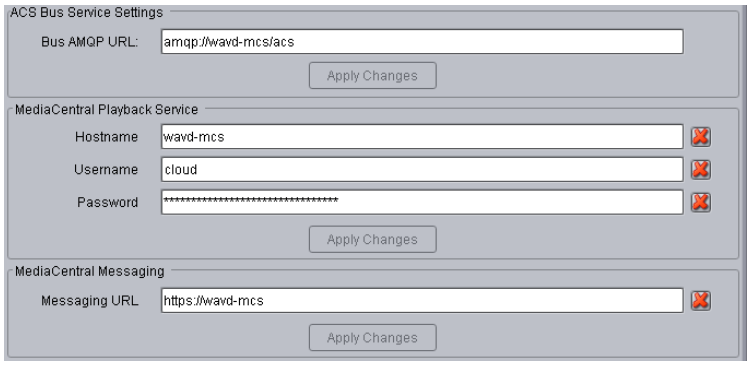
Decide upon the name of this custom user now. Suggested user name: **cloud**

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

Adjusting Interplay Production Settings

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

1. Launch the Interplay Administrator on the Interplay Engine. This can be found at: Start>Avid>Avid Interplay Access Utilities>Avid Interplay Administrator
2. Log 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 a Media Creation Workspace is selected.
4. Click Apply.
5. From the main menu, select Site Settings > MediaCentral and Platform Services Settings.



***Note**: 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:

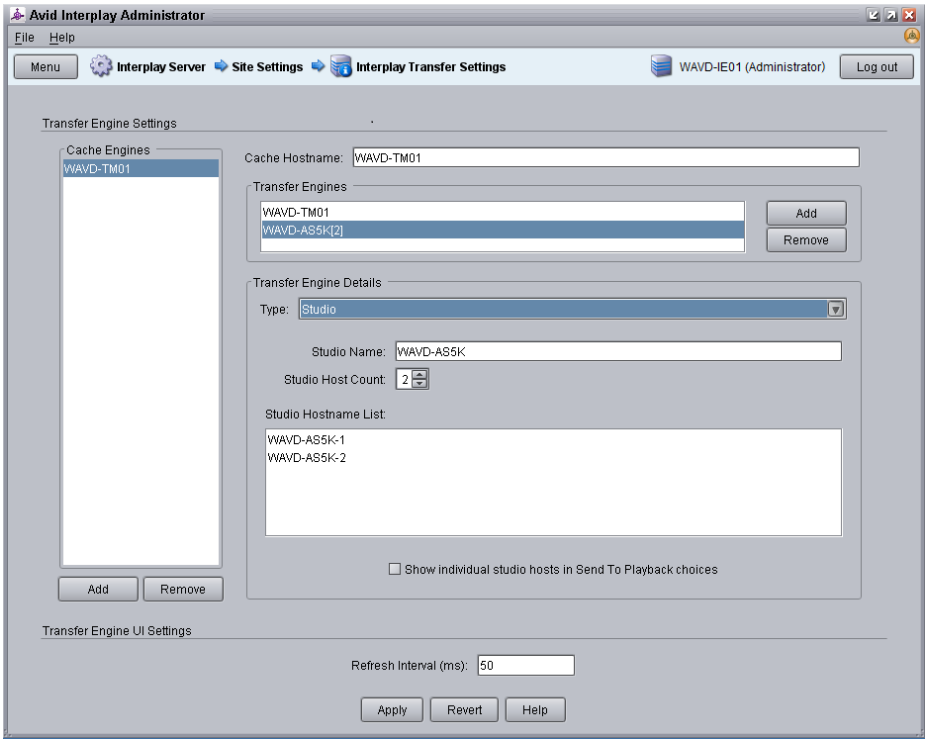
a. ACS Bus Service Settings: This feature is used in conjunction with Media Index configurations. For more information, see the *Avid Media | Index Configuration Guide*.

b. MediaCentral Playback Service (Cloud workflow only):

- Hostname: Enter the hostname of the MCS server. In the case of a cluster, enter the virtual hostname 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 Messaging: This setting enables a messaging workflow between MediaCentral UX and Media Composer. Enter the hostname of the MCS server in the form of a URL. In the case of a cluster, enter the virtual hostname 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.



9. Click Apply.

Verifying Interplay Production Media Indexer Configuration

MCS v2.5 and higher 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 **Appendix C: Configuring iNEWS for Integration with MediaCentral** for instructions on adding the version number to iNEWS.

Installing the MediaCentral Distribution Service

The MediaCentral Distribution Service (MCDS) is a lightweight 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.

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.
  - o 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 at: http://avid.force.com/pkb/articles/en_US/readme/Avid-Interplay-Production-V3-3-x-Documentation
  - o 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 Provider, Interplay Transfer Engine, etc.
- ☐ Must be installed on a system that has the ISIS 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 cannot be installed on an Interplay Production Transcode provider or STP Encode provider. This limitation has been resolved for MCDS v3.4.

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

Installing the MediaCentral Distribution Service:

1. Launch the MCDS installer on your desired system(s).
2. Proceed through the installation and accept the defaults.
   You may be asked to install prerequisite requirements such as Microsoft Visual C++.
3. Once installed, use Windows Computer Management to verify that the “Avid Interplay Central Distribution Service” is “Started” and the Startup Type is configured as “Automatic”.

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. For this procedure you require the following items:

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

> ***Note:*** *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).*

Note: *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.

Note: *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 inserted, make sure you choose the right one when performing this procedure.*

Preparing the Installation Drive for the HP ProLiant Gen9

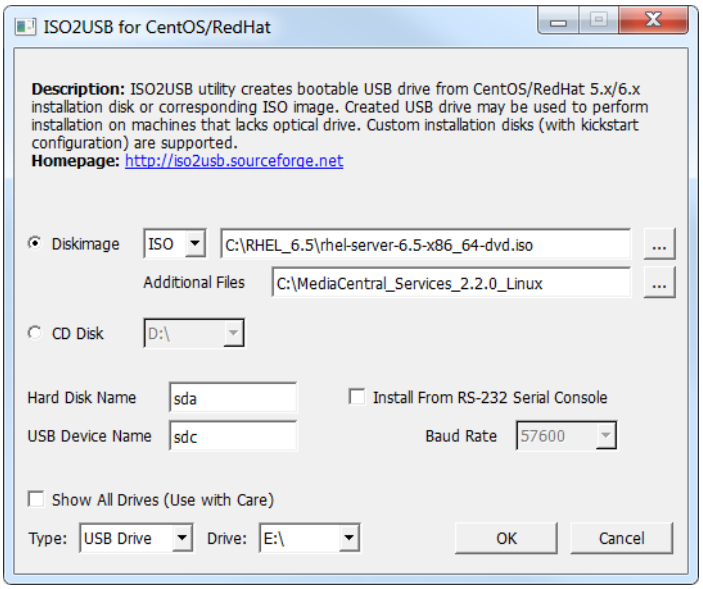
The procedure for creating the MCS installation drive on a ProLiant Gen9 server differs from that of other installations. Make sure you follow the customized instructions for your server type.

This section contains three procedures:

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

Preparing the MCS Installation USB Drive:

1. Log 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.



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).

   Note: *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

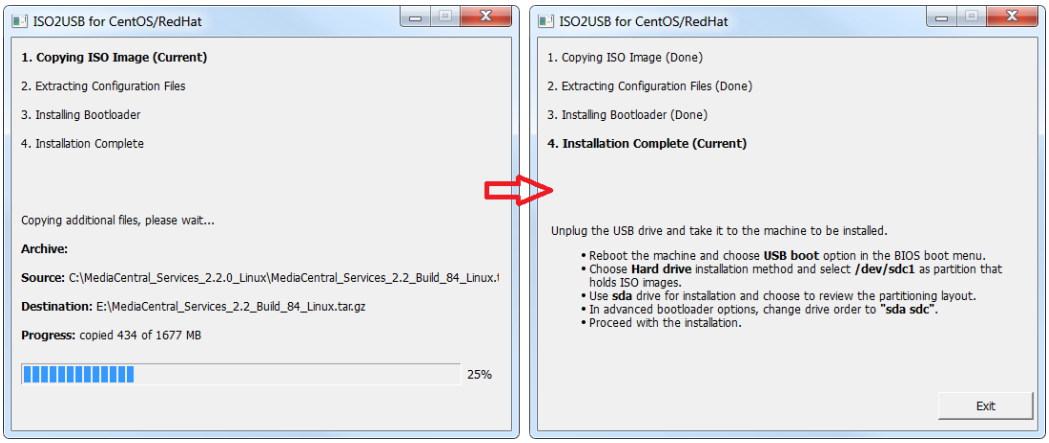
   Important*: For those familiar with earlier HP servers, the HP ProLiant Gen9 server identifies the RAID 1, RAID 5, and the USB drive with different device names.*

   Note: *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.



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

Note: *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.

Copying the 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** 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

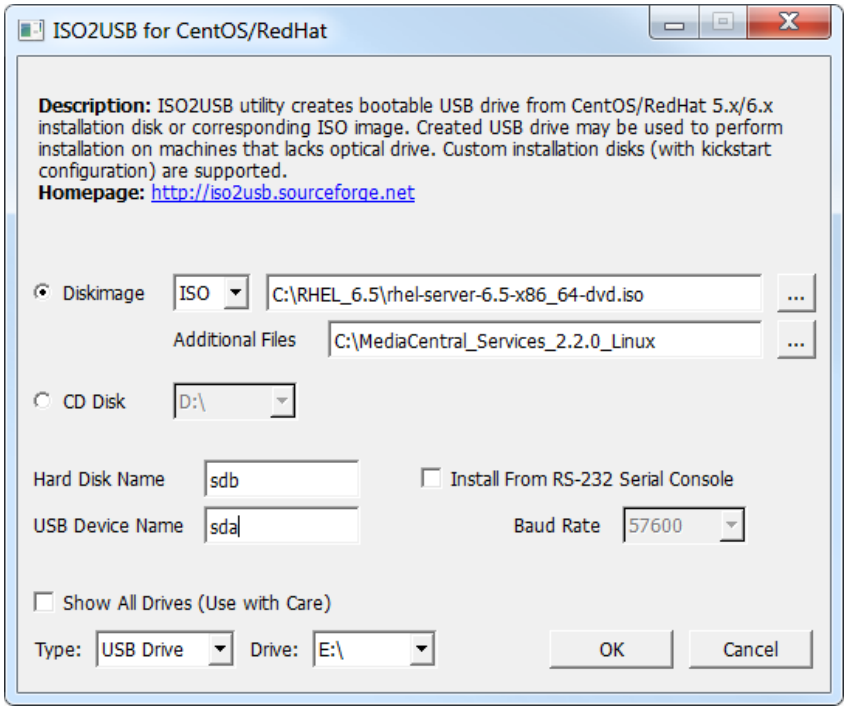
   Renaming the driver ISO is essential, since the installation script attempts to mount the first ISO it finds as the RHEL ISO. If you do not rename it, the installation will fail.

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.

Preparing the MCS Installation USB Drive:

1. Log 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.



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).

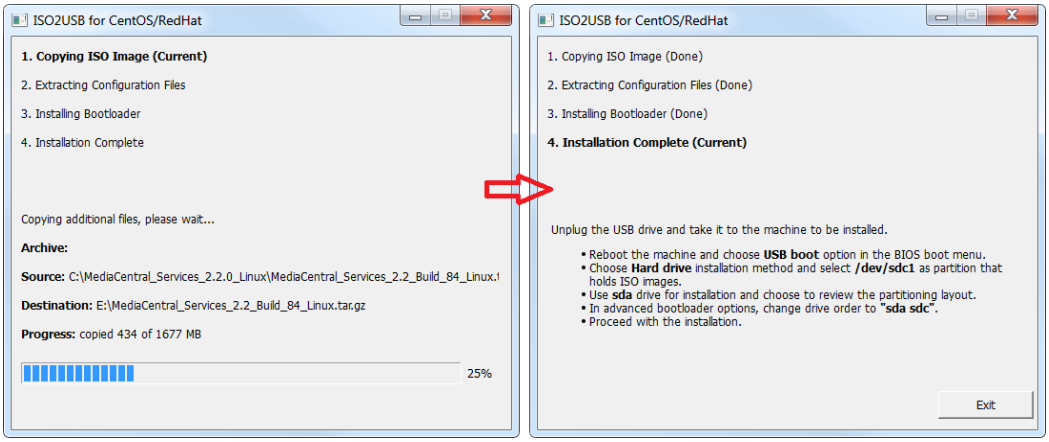
   Note: *Make sure the RHEL image (.iso) file is accessible locally (preferable) or over the network from your computer.*

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

   Note: *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.



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

Note: *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.*

PART II: BIOS & 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** 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	15 min
2	**Configuring the Onboard RAID** 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	varies

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

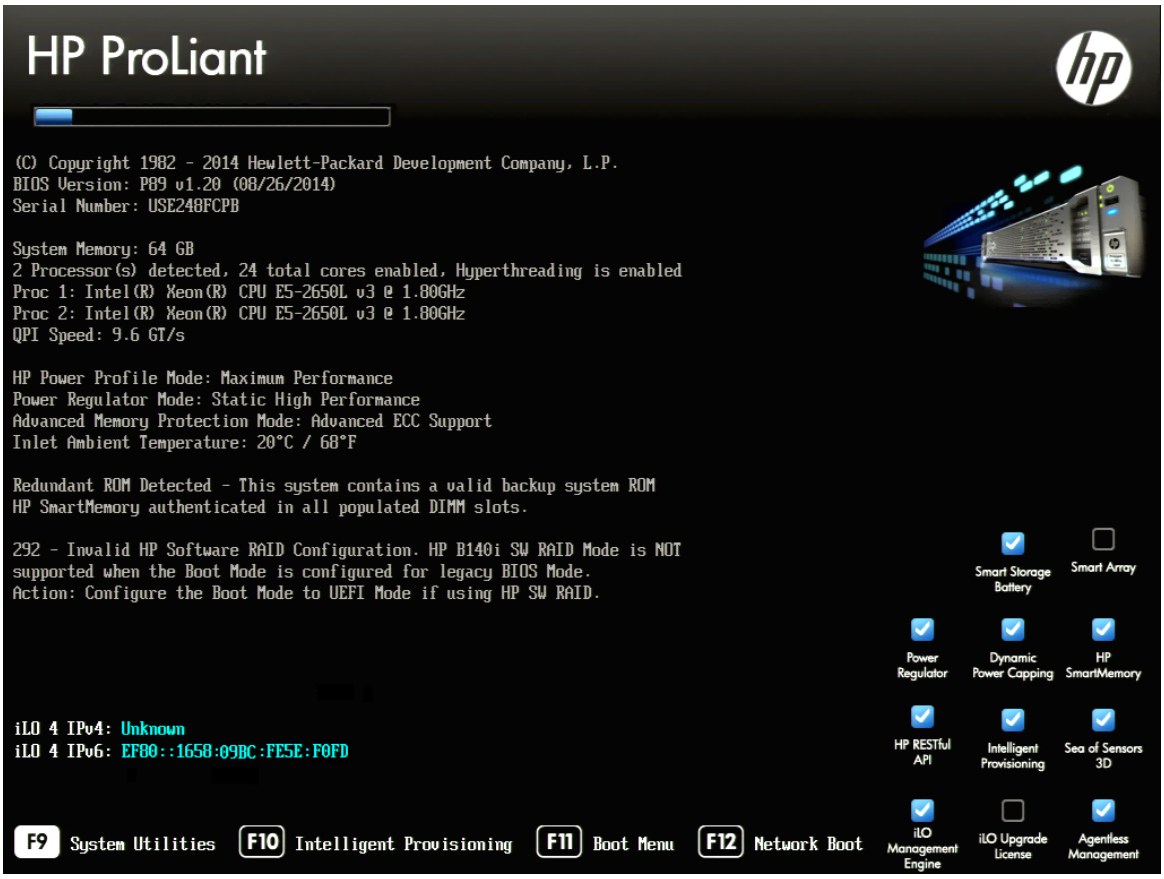
Servers are frequently shipped with BIOS settings configured for a power-saving mode. MCS makes intensive use of the server's CPUs and memory, especially when under heavy load. Configuring the server to operate at maximum performance will ensure operational efficiency.

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.

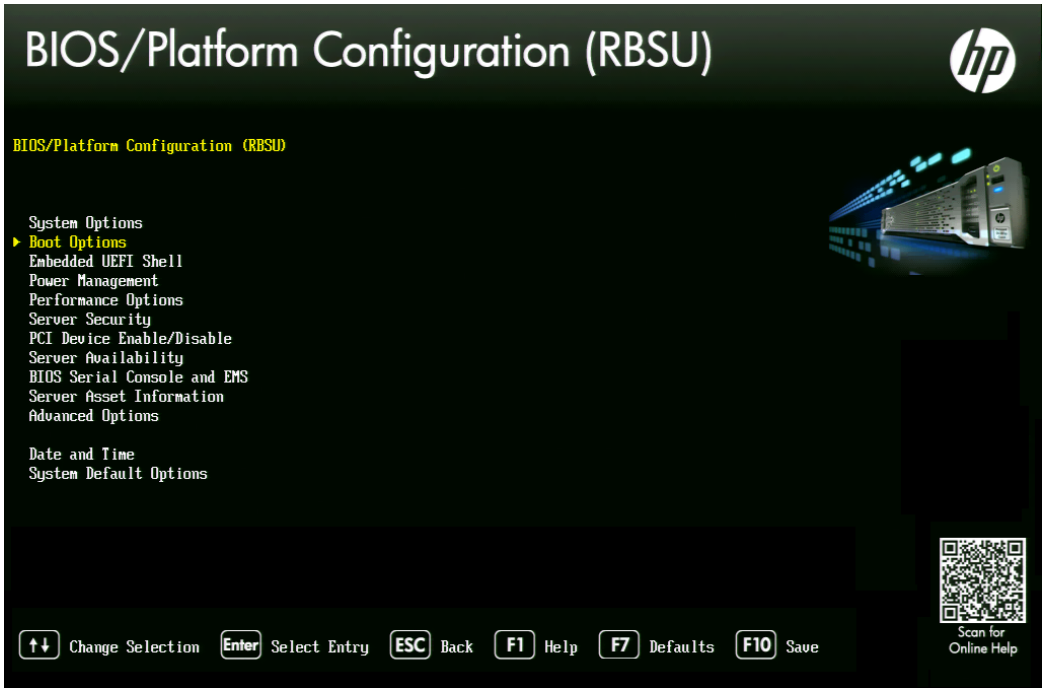
Configuring the BIOS on the HP ProLiant DL360 Gen9

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:

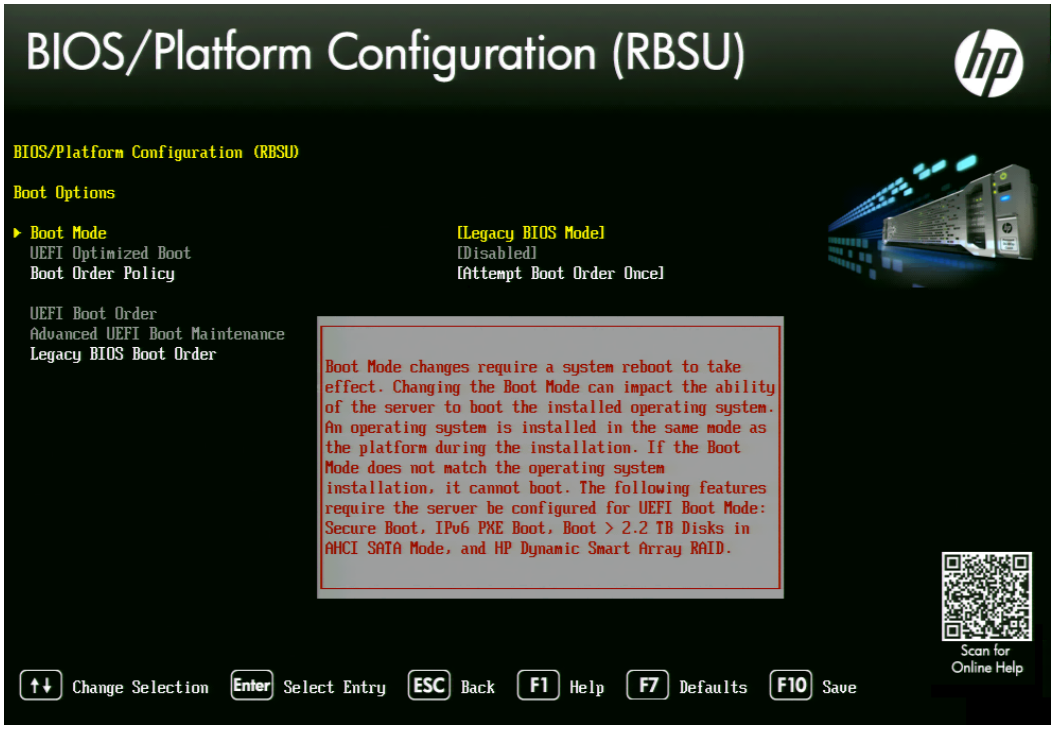


3. Select the **System Configuration** menu item and press Enter.
4. Select the **BIOS/Platform Configuration (RBSU)** menu item and press Enter.

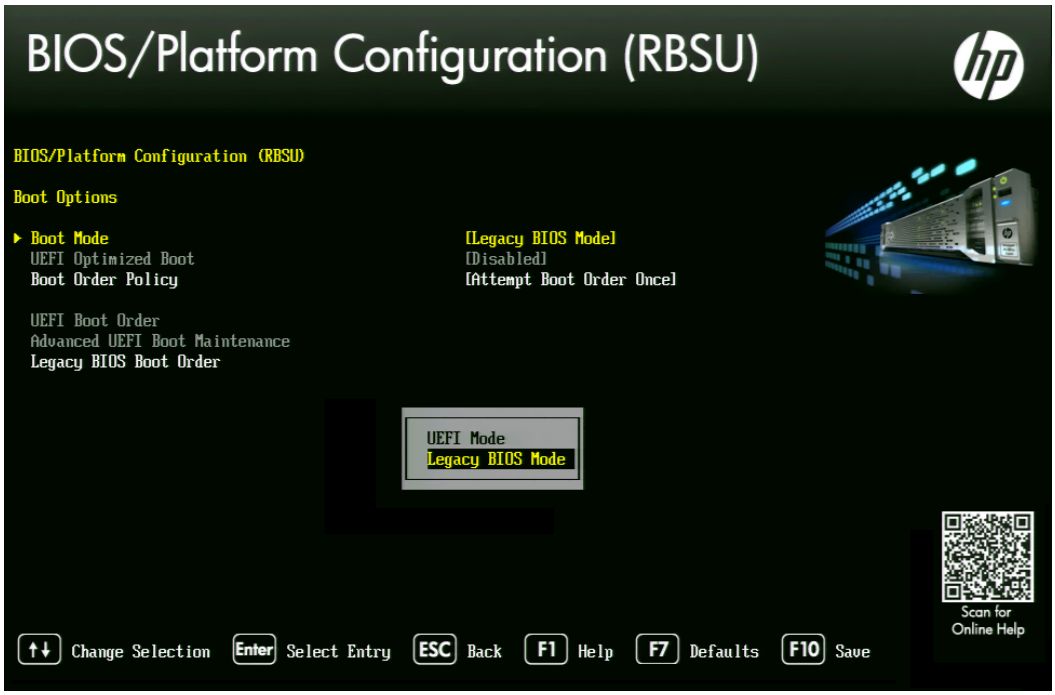


5. Select the **Boot Options** menu item and press Enter.
6. Select the **Boot Mode** menu item and press Enter.

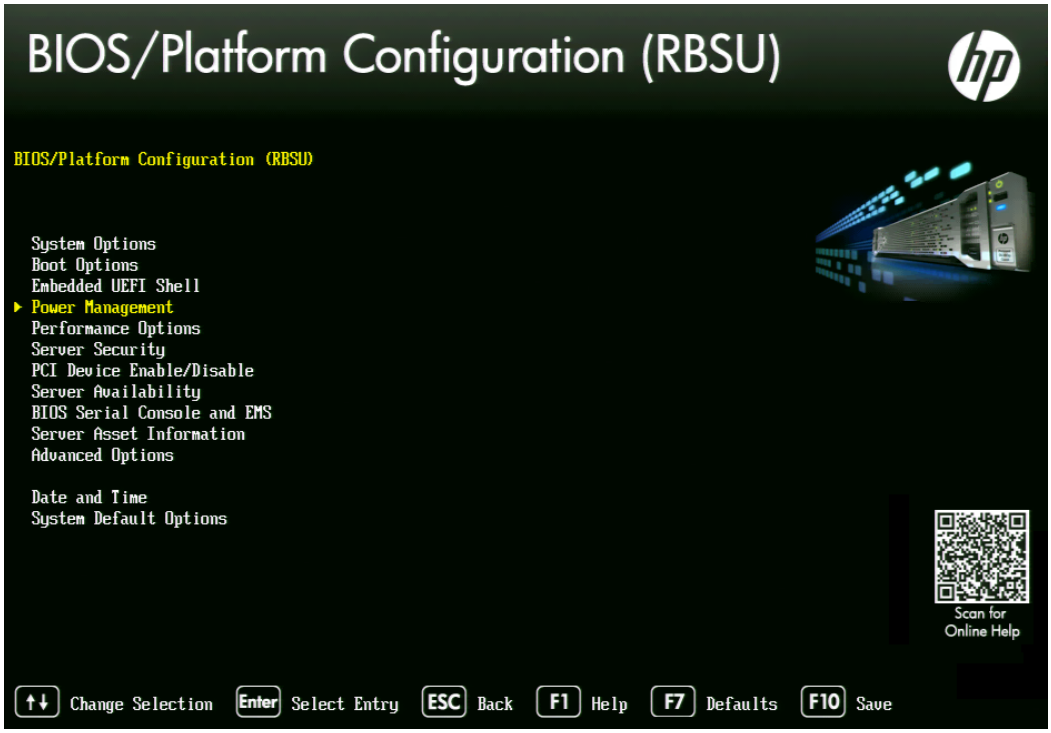
   You may see a warning message (shown below) indicating that Boot Mode changes will require a reboot. Press Enter to acknowledge this message.



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

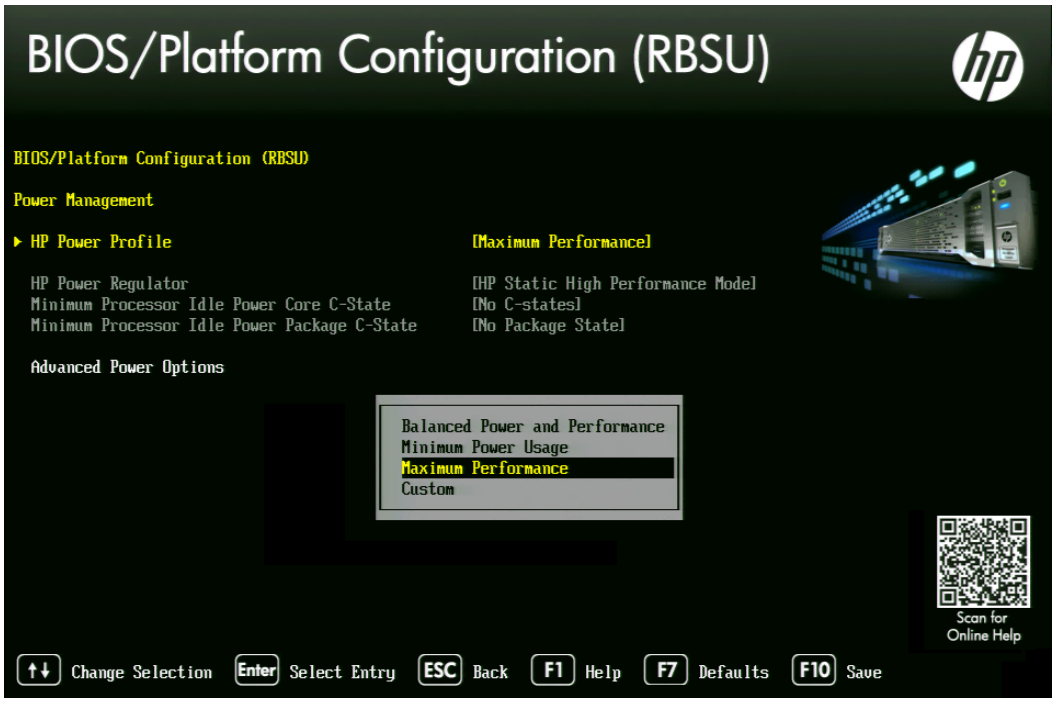


8. Press ESC to navigate back to the **BIOS/Platform Configuration (RBSU)** screen.
9. Select the **Power Management** menu item and press Enter.

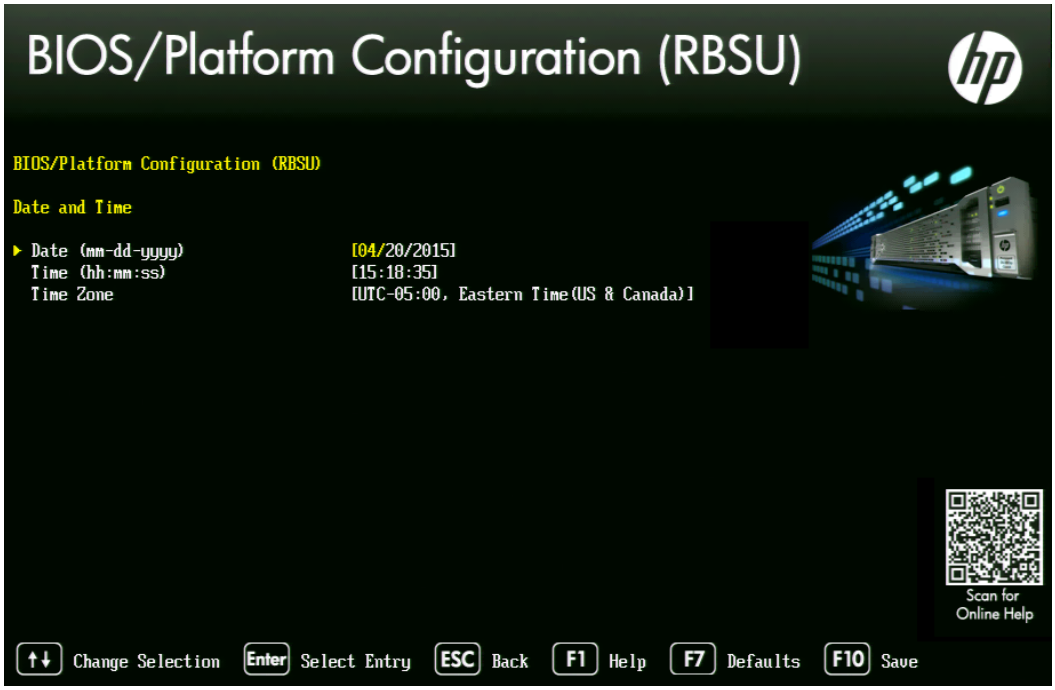


10. Press Enter to select **HP Power Profile**.

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



12. Press ESC to navigate back to the **BIOS/Platform Configuration (RBSU)** screen.
13. Select the **Date and Time** menu item and press Enter.



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.

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

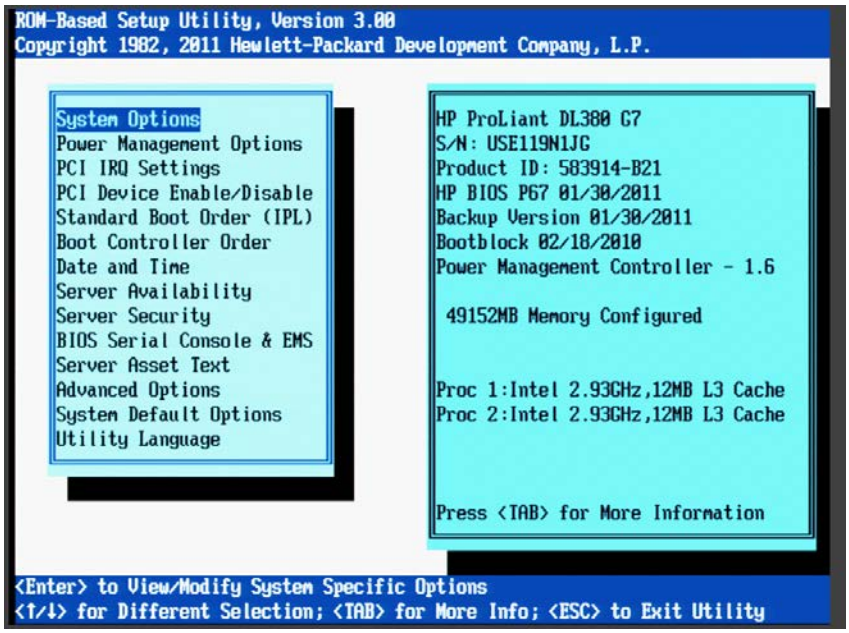
    The server reboots with new options.

Proceed to Configuring the Onboard RAID on page 43.

Configuring the BIOS on the HP ProLiant DL360p Gen8

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.



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.

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

8. Press Enter to save the changes and return to the Setup Utility menu.
9. Exit the Setup utility. Press Esc and F10 to save.

   The server reboots with new options.

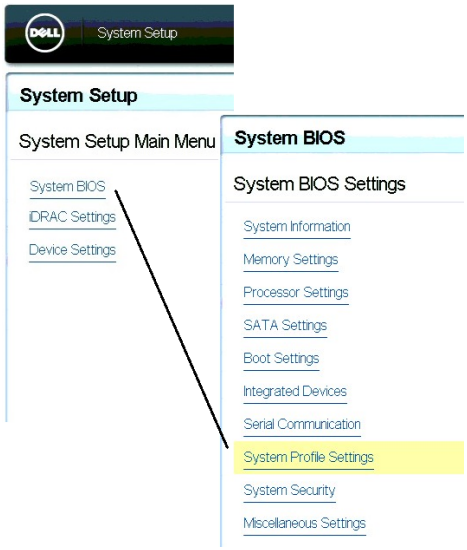
Proceed to Configuring the Onboard RAID on page 43.

Configuring the BIOS on the Dell PowerEdge R620 / R630

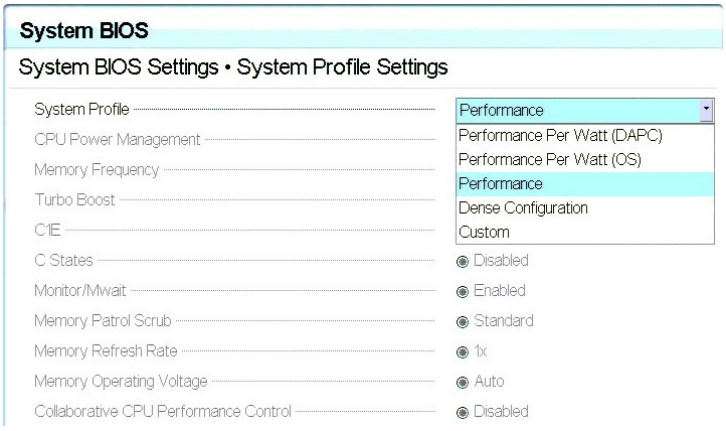
This process includes steps to ensure your MCS Installation USB drive is first in the boot order. Prior to beginning this process, ensure your MCS Installation drive is available.

For instructions on creating the boot drive, see **Preparing the Installation Drive for HP Gen8 and Dell Servers** on page 31.

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**.



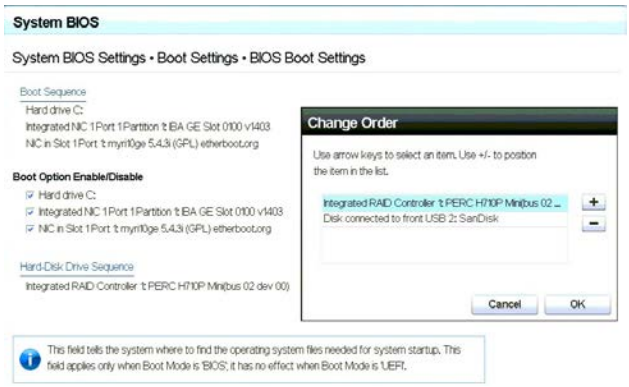
6. Select the **Performance** profile from the pull-down menu and click Back.



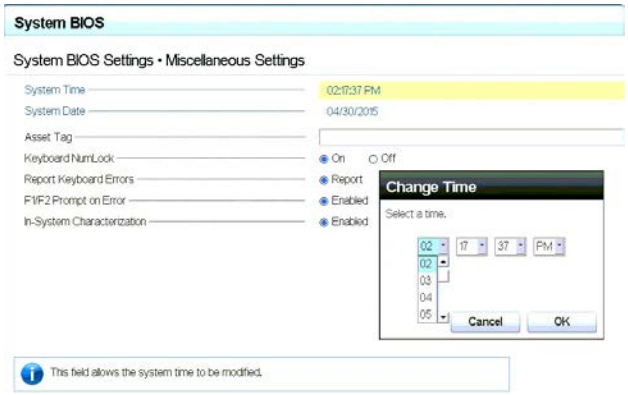
***Note**: There are three "Performance" profiles. Once of them specifically says "Performance" and not "Performance Per Watt."*

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.



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



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.

Note: *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 43.

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.

See the *MediaCentral Platform Services Concepts and Clustering Guide* for more information on RAID configurations.

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.

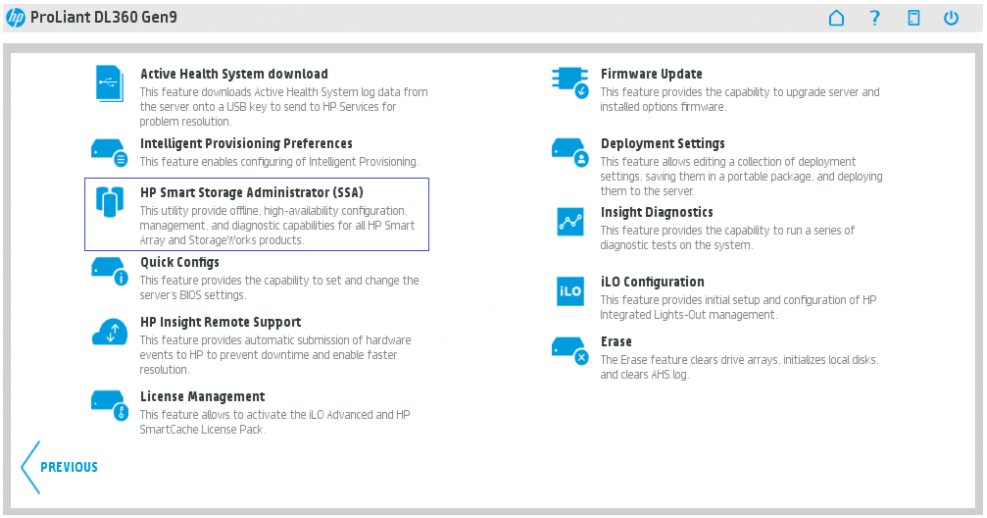
> ***Note:*** *If the list of available disks does not appear as expected, it may be that a RAID has already been created. Deleting a RAID destroys all the data it contains, so verify it is safe to do so first.*

> ***Note****: 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.*

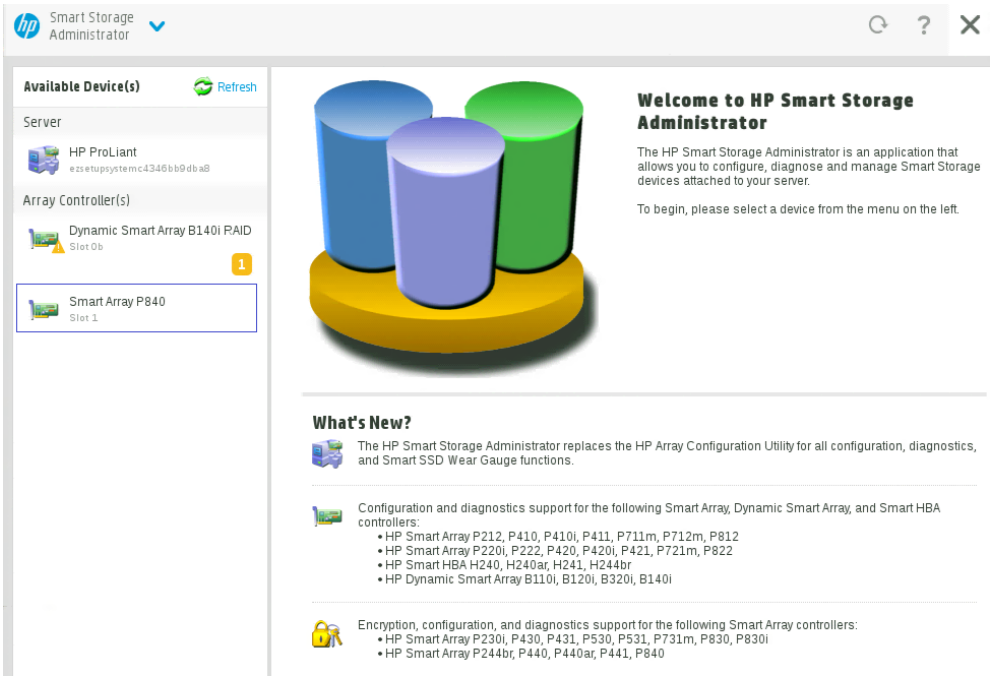
Configuring the HP ProLiant DL360 Gen9 RAID 1

Note: *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.*

1. Reboot the server and press **F10** to select **Intelligent Provisioning**.
2. Select **Perform Maintenance**.
3. Select **HP Smart Storage Administrator (SSA)**

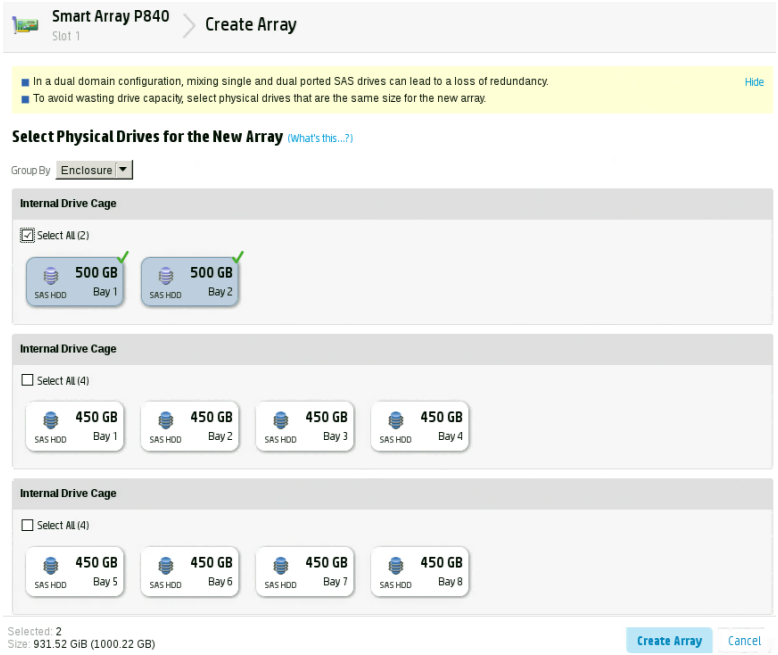


4. At the "Welcome to HP Smart Storage Administrator" screen, select **Smart Array P840** from left side menu.

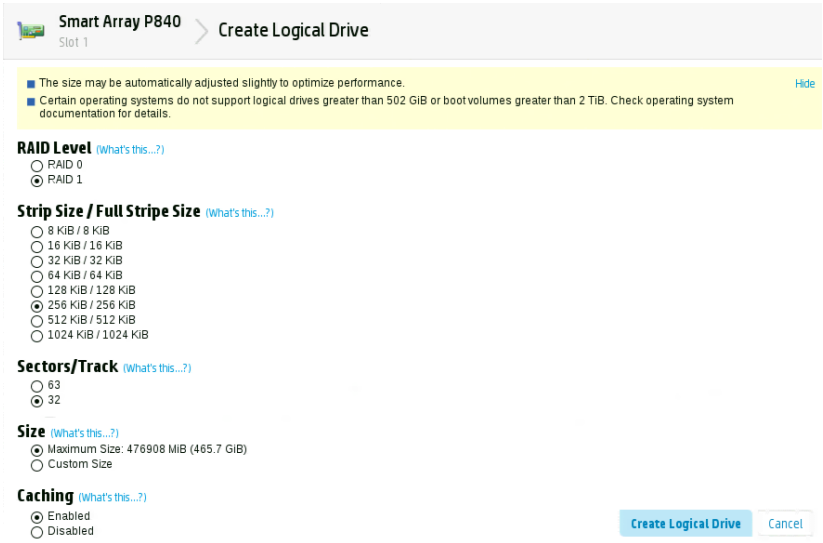


5. Select **Create Array** under "Actions".

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



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



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.

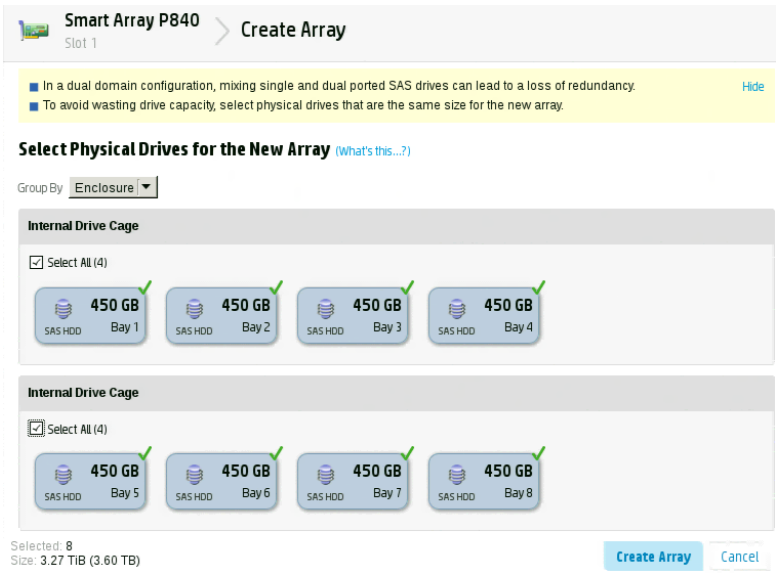
***Note**: Do not press the Escape key to exit, since this reboots the server.*

If applicable, proceed to **Configuring the HP ProLiant DL360 Gen9 RAID 5** on page 46.

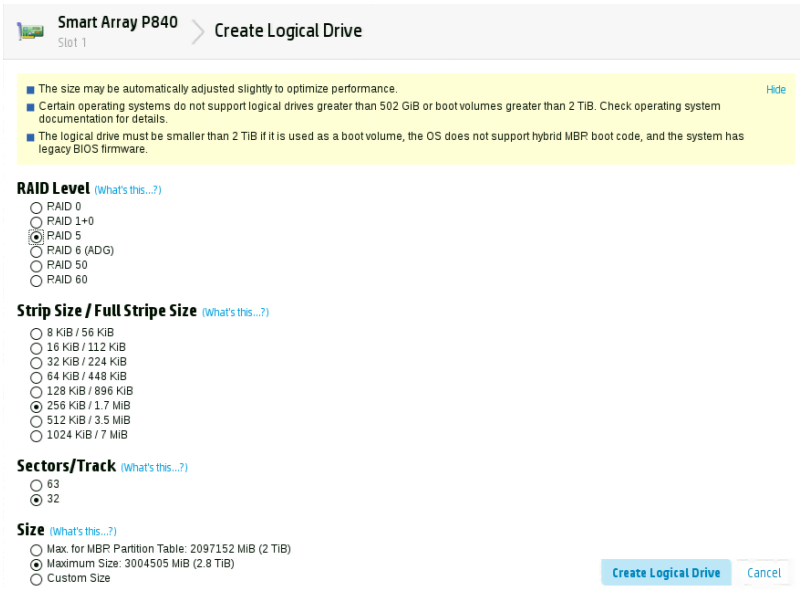
Configuring the HP ProLiant DL360 Gen9 RAID 5

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

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



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



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 **Installing RHEL and the MCS Software** on page 57.

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.

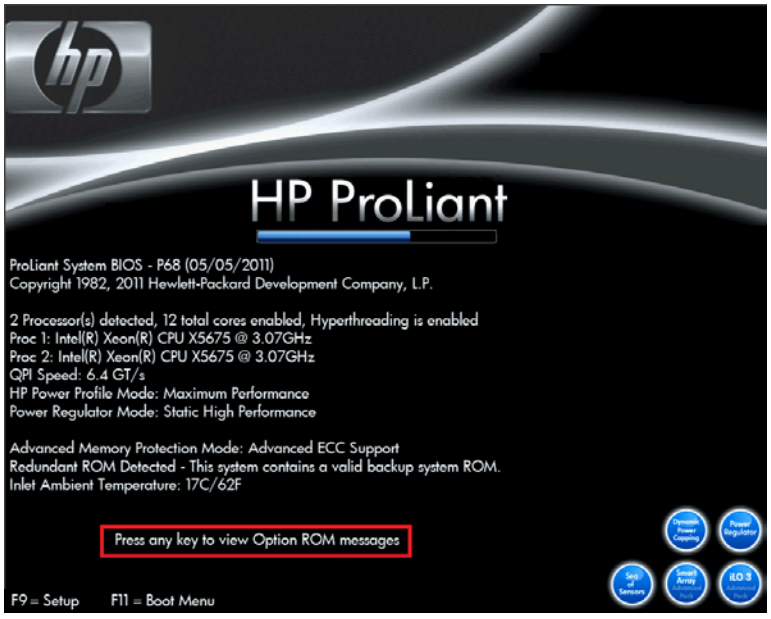
If applicable, configure the remaining HD drives in the server enclosure as a RAID Level 5. In a RAID 5, data is automatically distributed across all the disks in the RAID for increased performance and redundancy. This is done using the Option ROM Configuration for Arrays utility, in the HP server's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

> ***Note:*** *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.*
>
> ***Note****: 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****".*

Configuring the HP ProLiant DL360p Gen8 RAID 1

Note: *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.*

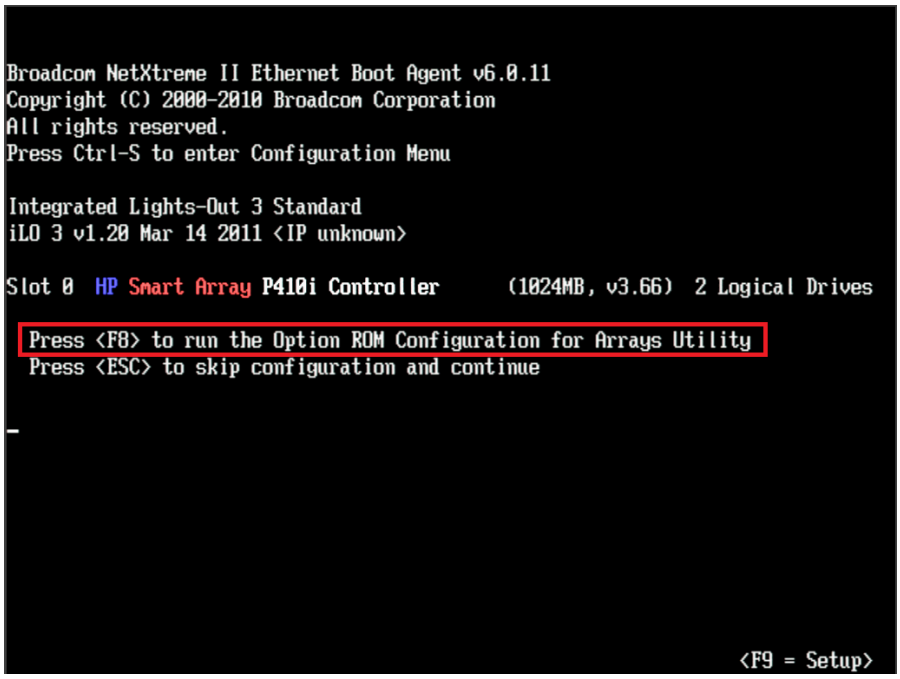
1. Reboot the server and press any key (**spacebar** recommended) when prompted to display the HP ProLiant "Option ROM" messages.



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

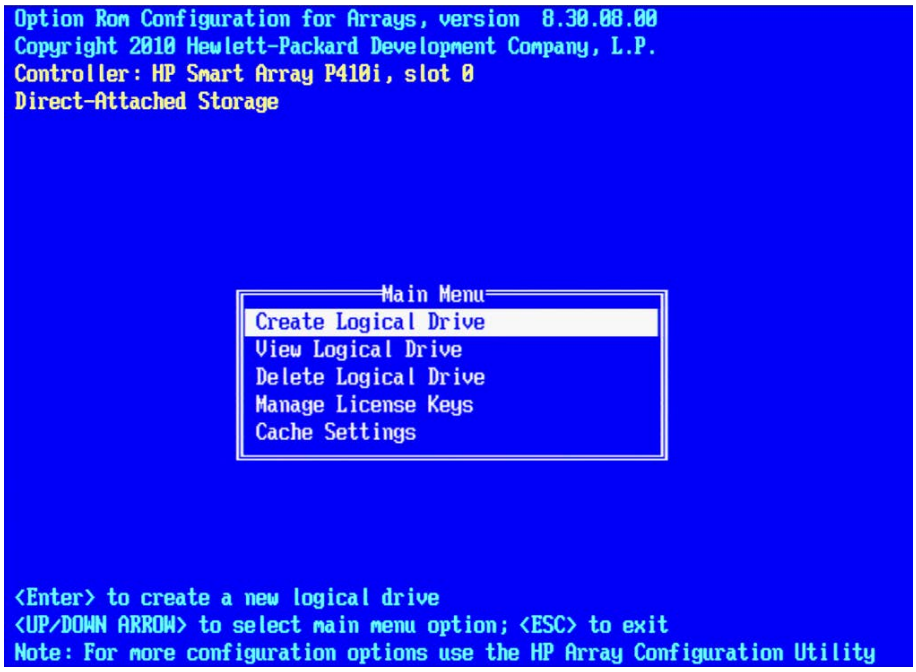
Detailed messages now appear as the server boots up.

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

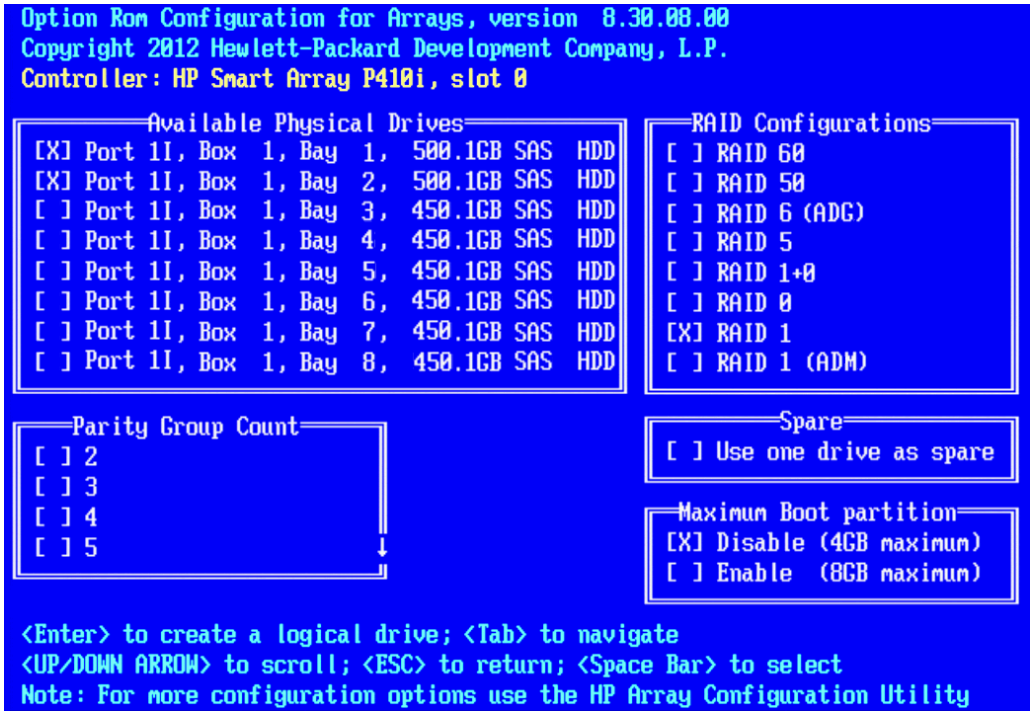


***Note**: The prompt to press **F8** can flash by quite quickly. If you miss it, reboot and try again.*

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



4. Select the following two HD drives in “Available Physical Drives”:
   - Box 1, Bay 1
   - Box 1, Bay 2



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

   ***Note**: 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.

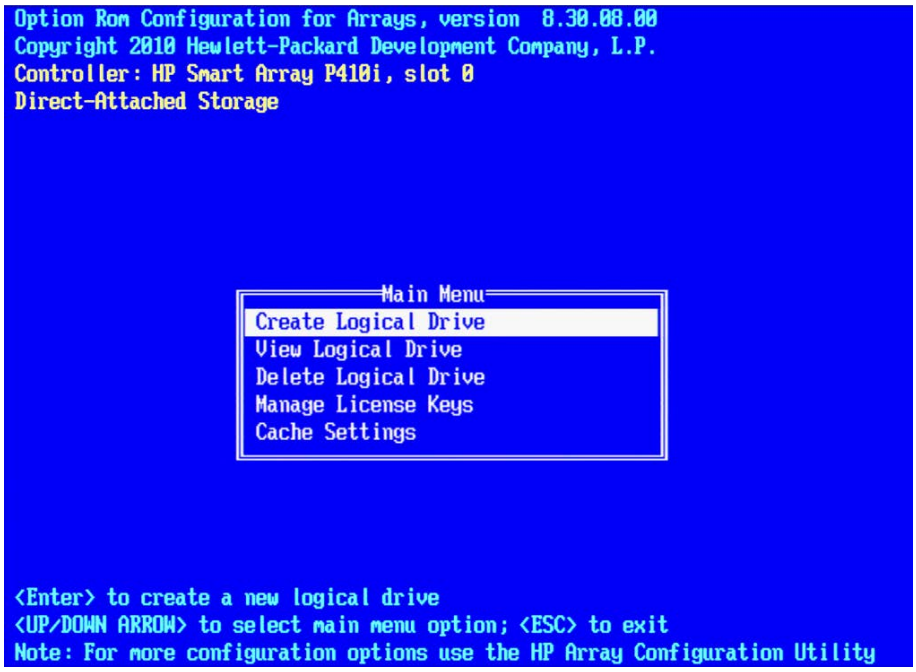
***Note**: Do not press the Escape key to exit, since this reboots the server.*

If applicable, proceed to **Configuring the HP ProLiant DL360p Gen8 RAID 5** on page 50.

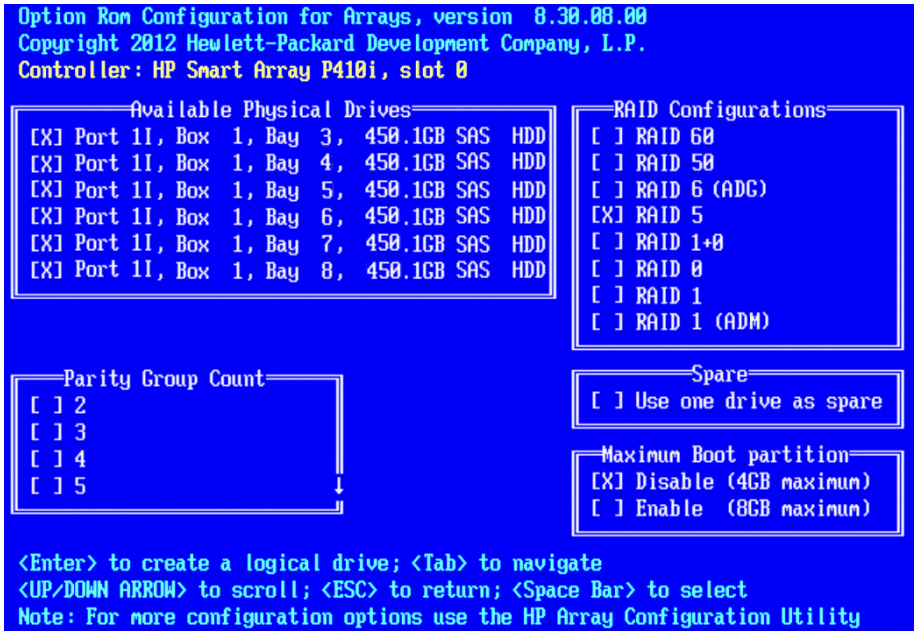
Configuring the HP ProLiant DL360p Gen8 RAID 5

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

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



2. Select the drives to be included in the RAID 5 in the “Available Physical Drives” section.
   - Box 1 Bays 3-8 (typical configuration)



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 **Installing RHEL and the MCS Software** on page 57.

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.

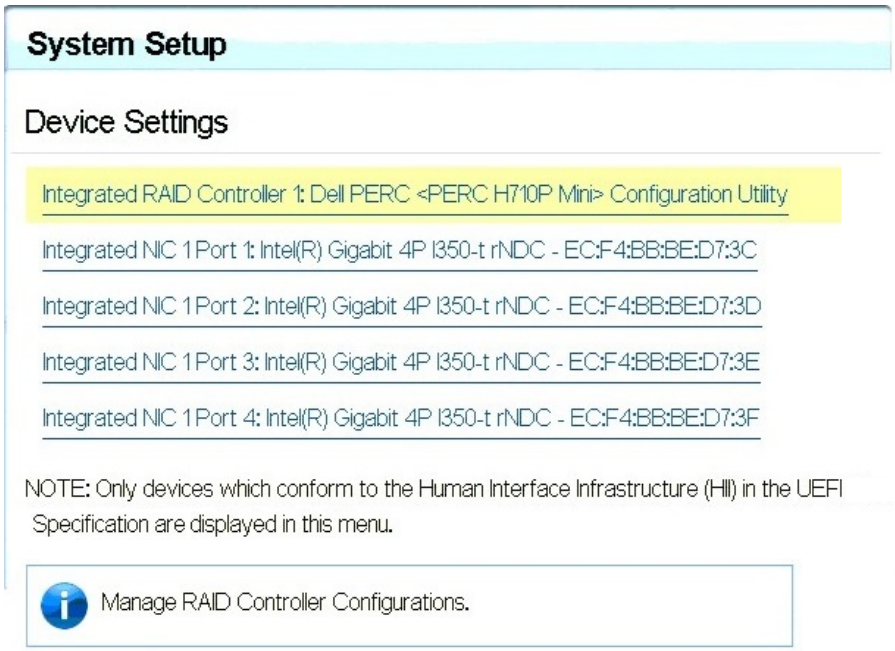
If applicable, the remaining drives in the server enclosure will be configured as a RAID Level 5. In a RAID 5 data is automatically distributed across all the disks in the RAID for increased performance and redundancy.

> ***Note**: 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**".*

Verifying the PowerEdge Dell R620 / 630 RAID Configuration:

***Note:** 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.*

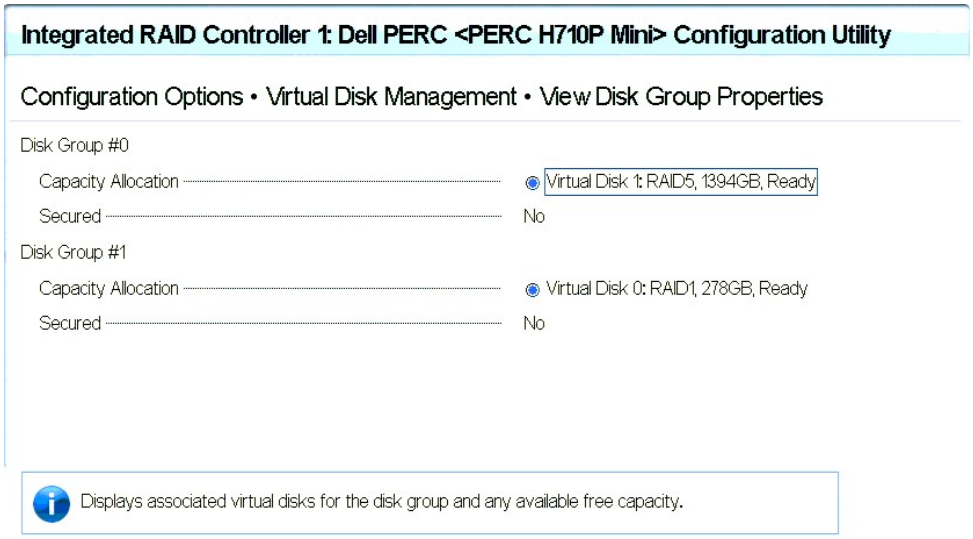
1. (if necessary) Reboot the server and press F2 to enter the BIOS.
2. From the main **System Setup** screen, select **Device Settings**.
3. From the **Device Settings** menu, select **Integrated RAID Controller Configuration Utility.**



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

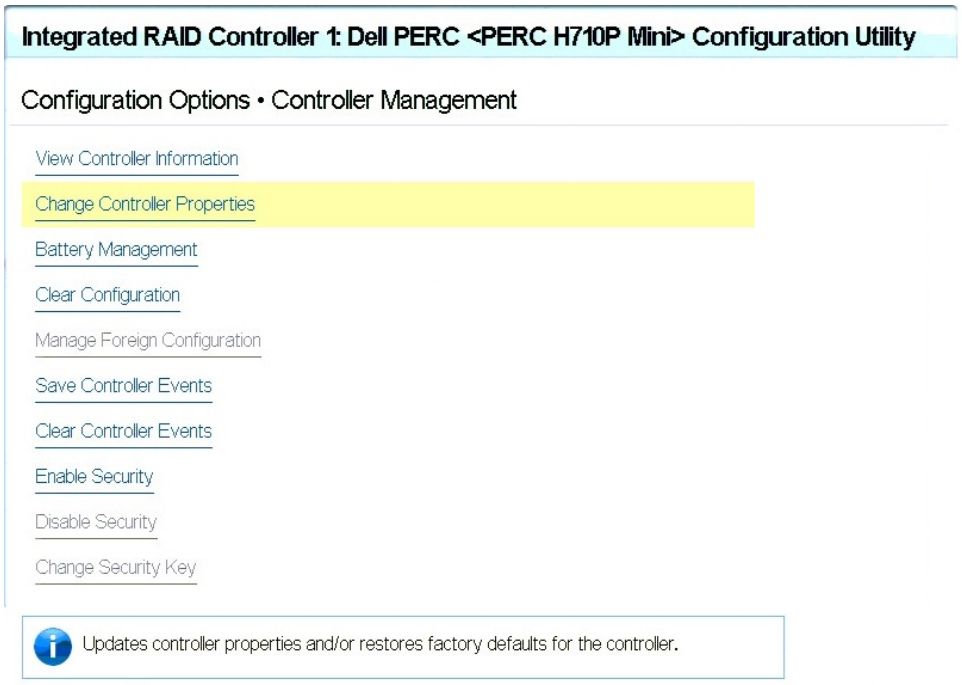
5. From the **Virtual Disk Management** menu, select **View Disk Properties**.

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

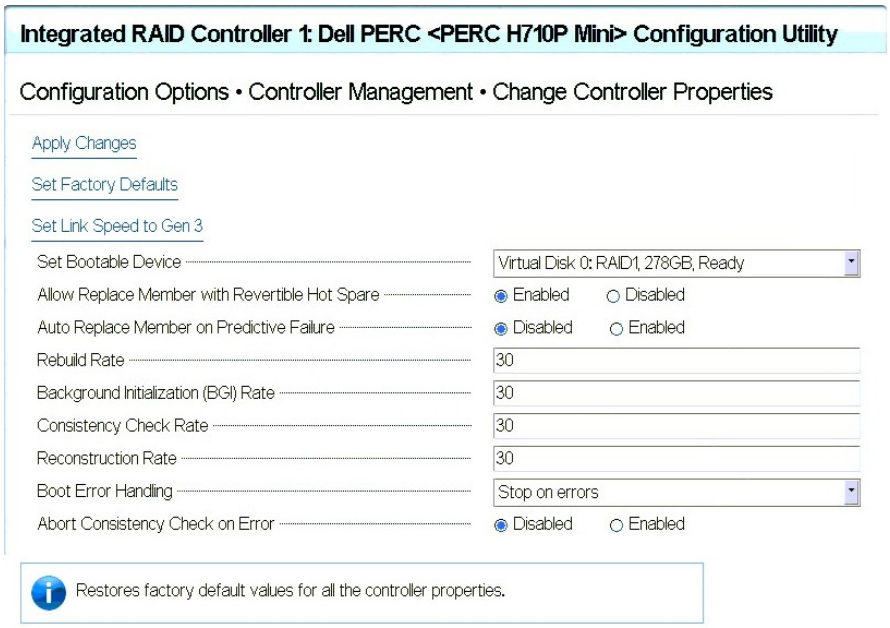


Note: *If the preconfigured RAID arrays do not exist, see* ***Working with the Dell RAID Controller*** *in Appendix A for information on creating the RAID.*

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



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



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

Proceed to **Installing RHEL and the MCS Software** on page 57.

PART III: SOFTWARE INSTALLATION AND PREPARATION

Chapter Overview

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

The following table describes the topics covered in this chapter.

Step	Task	Time Est.
1	Installing RHEL and the MCS Software	5 min
	Provides some introductory information on the installation process.	
2	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.	
3	MCS Software Deployment	30 min
	Covers the actual installation of RHEL and MCS.	
4	Booting RHEL for the First Time	5 min
	Covers keyboard layout configuration and a process for changing the default 'root' user password.	
5	Network Configuration	30 min
	Guides you through the configuration of all network-related settings.	
6	Configure Date and Time Settings	15 min
	Configuration of Date, Time, Time Zone and NTP settings.	
7	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.	
8	Enabling / Disabling 3G and Edge Streams	2 min
	Instructions for enabling / disabling 3G and Edge streams.	
9	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.	
10	Installing Security Updates	15 min
	Information regarding Security Updates for RHEL.	
11	Installing Software Patches	15 min
	A reminder to install available software patches.	
12	Upgrading the Avid Shared Storage Client Software	10 min
	In the event than an updated version of the ISIS Client software is required for your environment, client upgrade instructions have been provided.	

Installing RHEL and the MCS Software

This process will step you through the installation and configuration of an MCS server.

***Caution**: If you are in the process of upgrading from an earlier version of MCS — called ICS in earlier releases — it is a fresh install, and will overwrite your current ICS settings and databases.*

Before proceeding with the upgrade, back up your current settings:

- ☐ ***Database**: Save a copy of the ICS settings and database using the backup script (system-backup.sh) provided. See Backing up the MCS System Settings on page 163.*
- ☐ ***SSL Private Key(s)**: If you deployment makes use of CA-signed certificates, back up private(s), regardless of the upgrade path.*

***Note**: For details on upgrading to MCS 2.7 from an earlier release, see the MCS 2.7 Upgrade Guide, available on the MediaCentral Platform Services page of the Avid Knowledge Base.*

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 58 (the next page).
- ☐ If you are installing MCS on an HP server, proceed directly to **MCS Software Deployment** on page 62.

  ***Note:** Both processes use the MCS Installation USB drive to install RedHat and MediaCentral Platform Services. Earlier in this document, you created the USB installation drive using specific drive names (sda, sdb). 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."*

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.

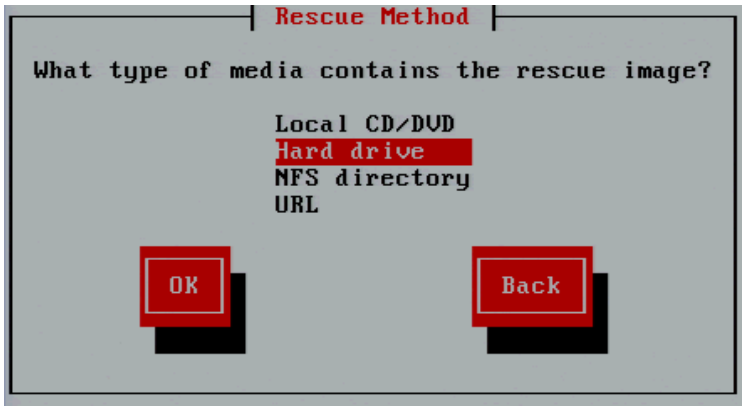
Deleting and recreating the RAID sets using the DELL BIOS utility does not erase data, nor does it delete existing partitions. That is, deleting a RAID does not delete the partition table — unless you initialize the disk at the same time. However, initializing the disk is a slow process.

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.

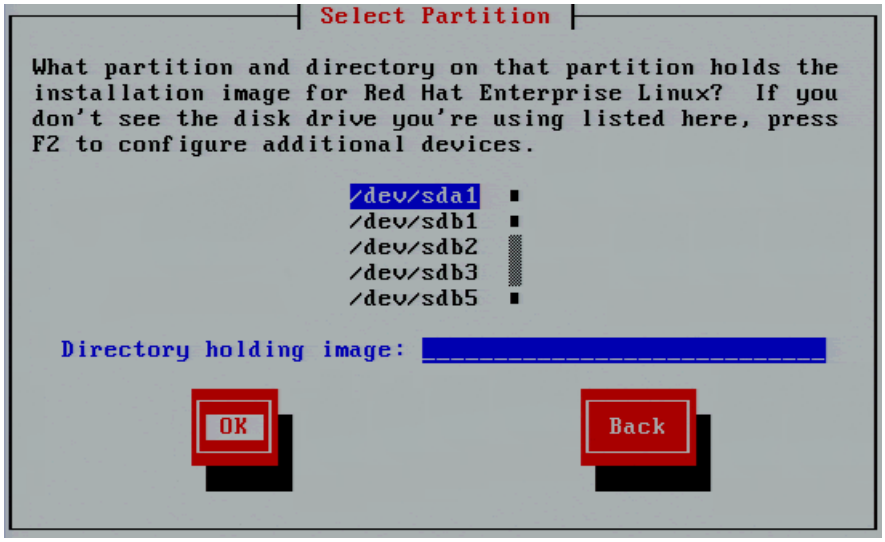
If you are installing MCS on an HP server, proceed to MCS Software Deployment on page 62.

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

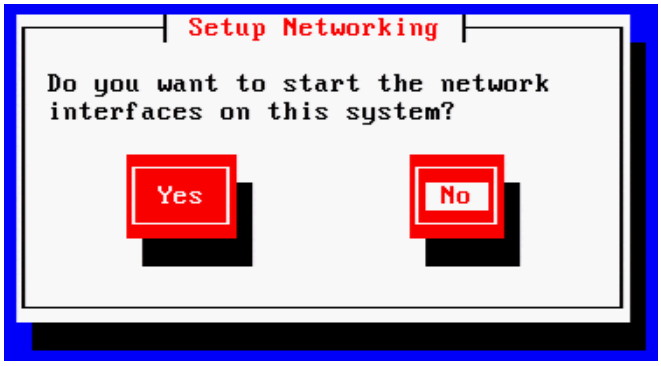
3. When prompted choose the language and keyboard.
4. Choose "Hard drive" as the rescue method. For the purposes of booting from a RHEL image, the USB drive is considered a hard drive.



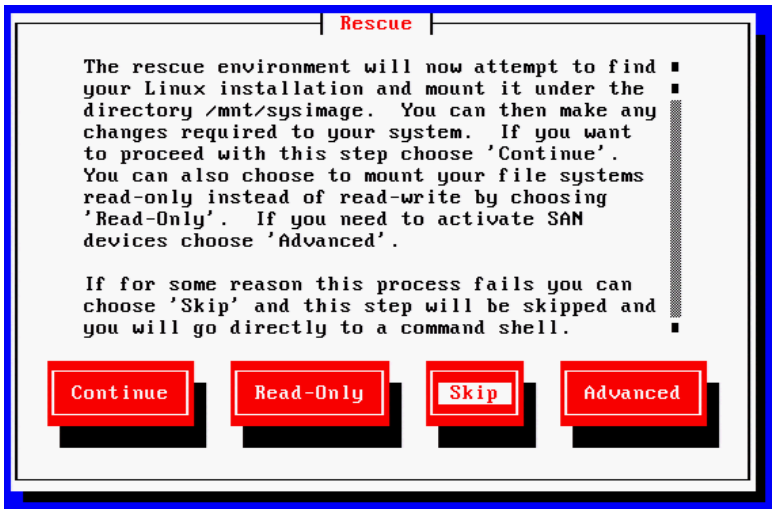
5. Select the “/dev/sda1” partition (the USB drive). Leave the “Directory holding image” field blank.



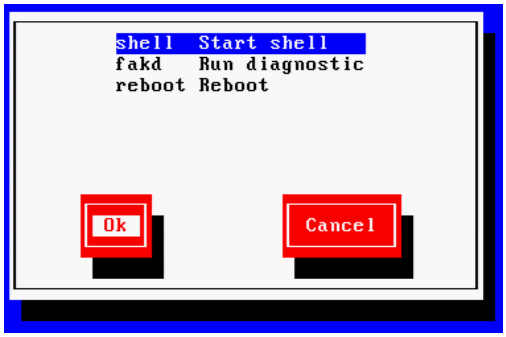
6. Select No in the Setup Networking window; as networking is not needed at this time.



7. Select “Skip” in the Rescue window.



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 filesystem (sdb4, sdb5) could be possible. 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. 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 62.

MCS Software Deployment

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

1. Ensure the MCS Installation USB drive is connected to the server and reboot if necessary

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

2. Wait for the RHEL Welcome screen to appear.

   Note*: 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.*

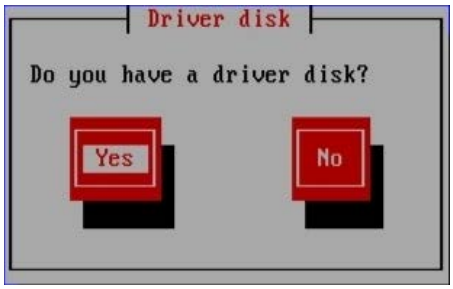
3. If you are installing on an HP ProLiant Gen9 server, install the RHEL driver to enable RHEL support for the storage controller before proceeding:

   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.



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**.

Note: *If you are upgrading your system, do not use the "Upgrade" option. For upgrading instructions, see the "MCS 2.7 Upgrade Guide".*

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

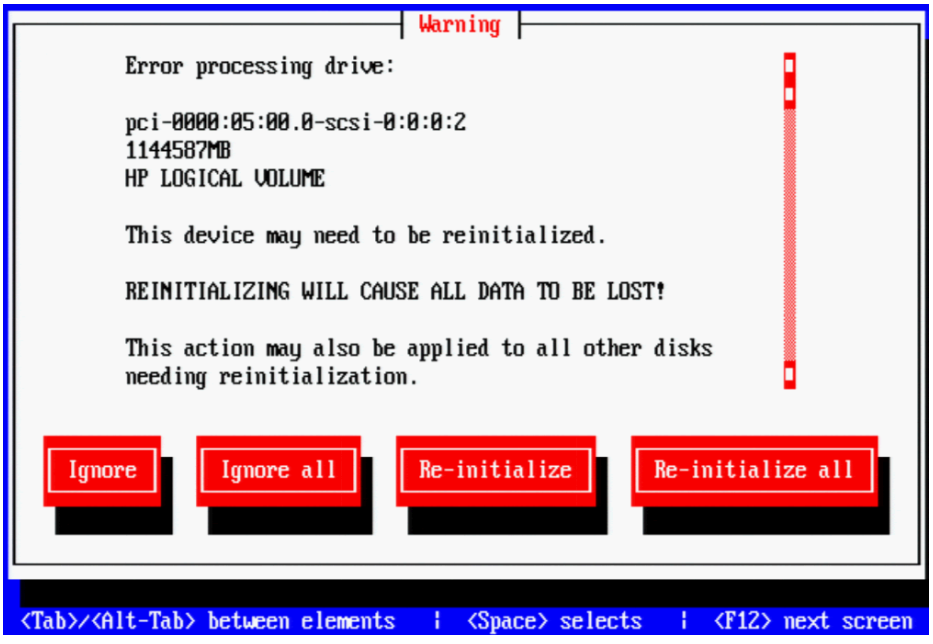
Note: *Regarding the following error message:*

```
Unable to download kickstart file
```

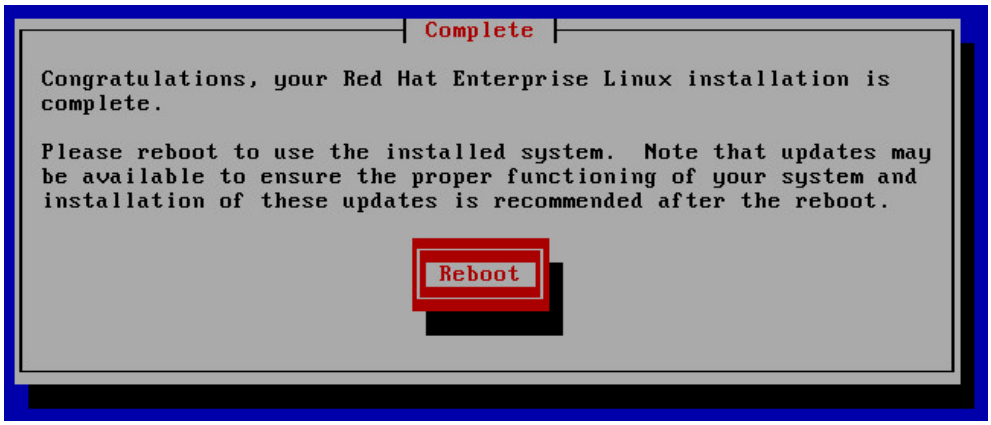
If you see this message, it could indicate that the partition where the installation program expects to find the kickstart file (sda) is already in use. The most likely cause is a KVM with "virtual media" capability reserving the sda partition to facilitate the mapping of removable drives to the attached server.

To resolve the issue, disable the virtual media capability. Alternately, unplug the KVM and connect to the server directly using an external monitor and USB keyboard.

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.



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



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

   Note: *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 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

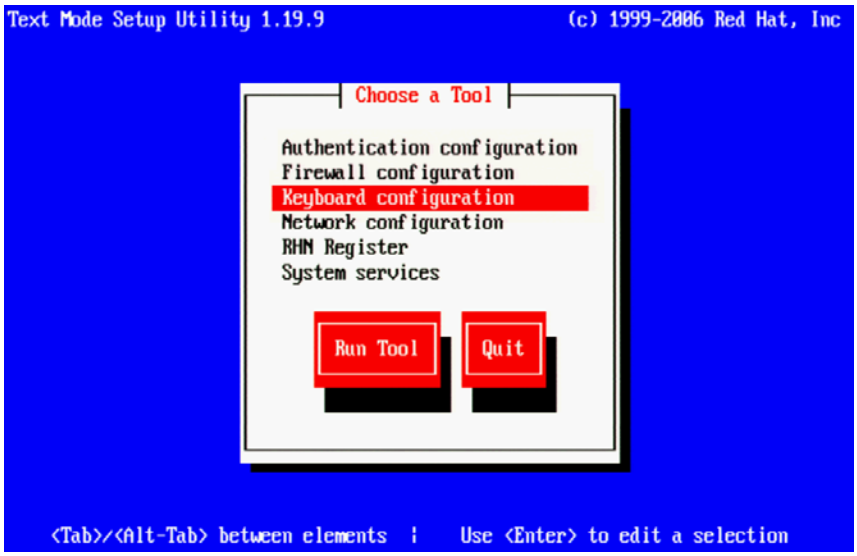
Like many operating systems, when you boot RHEL for the first time, you will be asked to provide some basic information. A RHEL "first boot" causes the RHEL Configuration screen to appear, providing access to system setup menus.

Note: *The first boot setup menu can be accessed at any time by typing "setup" (without quotes) at the Linux command prompt.*

Note: *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.*

Booting from the System Drive

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



2. In the Keyboard Selection menu, use the arrows to select the appropriate language for your keyboard.

   Note: *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.*

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.

The first boot setup menu can be accessed at any time by typing "setup" (without quotes) at the Linux command prompt.

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.

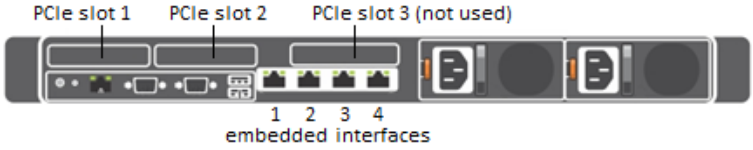
Network Configuration

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 **Appendix B: Configuring Port Bonding for Interplay MAM**.

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 "eth*x*", 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 "em*x*", 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).



Note: *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".*

Note: *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 onsite 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, a single- or double-dash distinguishes *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 **Ensuring the NIC Interface Comes Up at System Startup** on page 76.

   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 **Ensuring the NIC Interface Comes Up at System Startup** on page 76.

   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 “eth*x*”, additional steps need to be taken to ensure “eth0” is used.

To verify the NIC interface name:

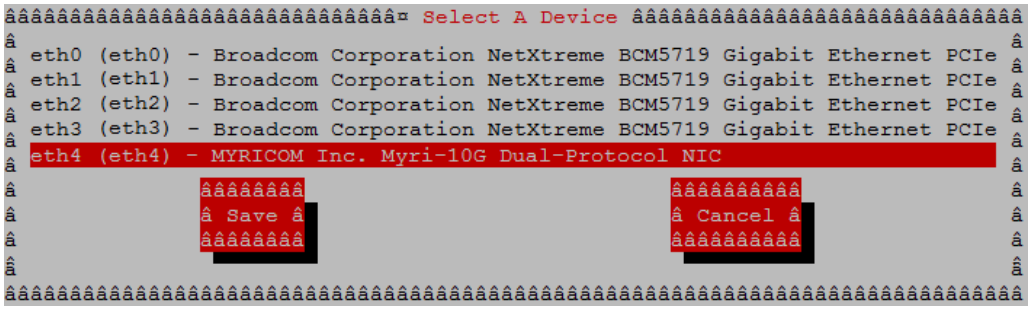
1. Enter the RHEL Configuration screens by typing the following at the command prompt:

   ```
   setup
   ```

2. From the Choose a Tool menu, select **Network Configuration**. Press **Enter**.

3. From the Network Configuration menu, select **Device Configuration**. Press **Enter**.

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



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 will need to rename it. You will also rename the NIC interface currently using the name “eth0”.

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

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

   Note: *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 output may look similar to the following. Note that in the example below, the 10Gb Myricom card has been assigned “eth4”. In this scenario, you will want to swap the names for “eth0” and “eth4” so that the desired Myricom board is renamed “eth0”.

```
# 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"
```

2. Locate the lines corresponding to the NIC card 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 append to the end of the line:

   `NAME="eth0"`

4. Change **NAME="ethX"** (e.g. *eth1*, *eth2*, etc.) to the following:

   `NAME="eth0"`

5. Locate the line corresponding to the NIC card that was already using the name eth0 and rename it:

   `NAME="ethX"`

   Where “X” is the number you removed in step 5 (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 NIC interface, you will also need to remove the hardware references – generally known as MAC addresses – from the affected NIC interface configuration files.

For each card where you renamed a NIC interface, edit the corresponding interface configuration file and remove the hardware identifier. Otherwise, Linux will override the changes you made earlier and reassign the old interface names the next time it boots (or you restart the Linux network services).

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 NIC 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 will refresh automatically after the reboot.

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

   Note: *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 will assume the configuration of a static IP address is desired.

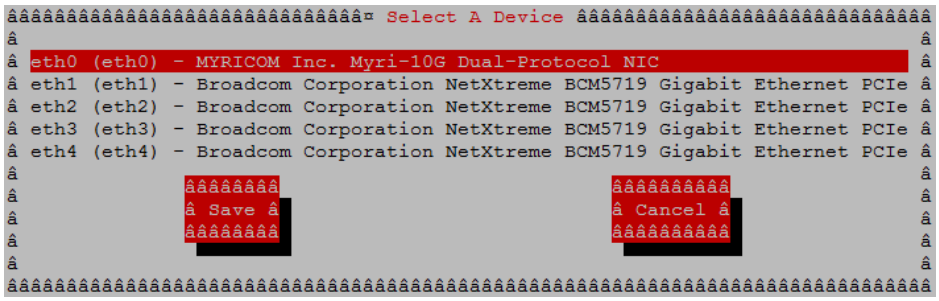
1. Enter the RHEL Configuration screens by typing the following at the command prompt:

   `setup`

2. From the ***Choose a Tool*** menu, select ***Network Configuration***. Press **Enter**.

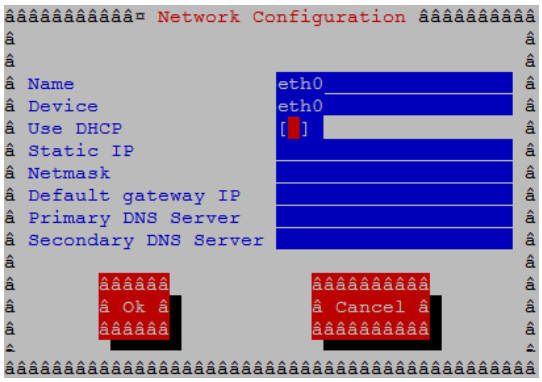
3. From the ***Network Configuration*** menu, select ***Device Configuration***. Press **Enter**.

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



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

   Note: *If you configured port bonding for an Interplay MAM integration, your primary interface may be called "bond0". For more information on port bonding, see Appendix B.*



5. Dynamic Host Configuration Protocol (DHCP) is the default option. Arrow down to the "Use DHCP" line and press the spacebar to deselect it.

6. Enter the following information:

   - ☐ Static IP address
   - ☐ Netmask (Subnet)

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

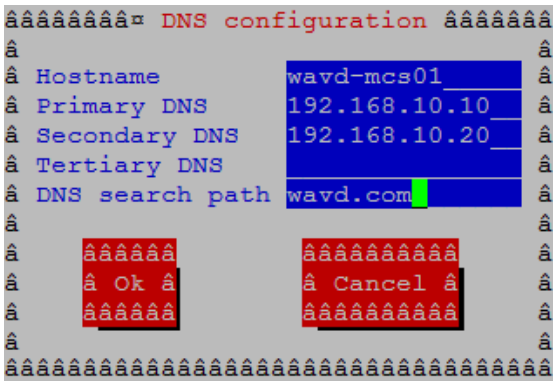
   - ☐ Default gateway IP
   - ☐ Primary DNS server
   - ☐ Secondary DNS server (if applicable)

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

   You are returned to the list of NIC cards in the enclosure.

8. Select Save and press Enter.

9. From the ***Choose a Tool*** menu, select ***DNS Configuration***. Press **Enter**.



10. Enter the following information for the DNS Configuration:

    ☐ Enter the 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.

    ***Note**: 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

11. Select Save & Quit. Press **Enter**.

12. 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**). 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.

1. Using the following command, 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
```

   ***Note**:* 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 will be configuring an MCS cluster, you will want to 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.

***Note**: 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

Verifying the resolv.conf file:

The resolv.conf file contains your DNS and domain information.

1. Verify the DNS Server information has been stored in the RHEL resolver configuration (resolv.conf) file:

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

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

   Using the vi editor, one or more additional search domains can be entered if necessary. 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
   ```

   ***Note**: Due to a caveat in Linux, if you do not delete the* resolv.conf.save *file, when you reboot, Linux overwrites the changes you just made.*

Verifying the nsswitch.conf file:

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.

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 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, verify that the primary network interface is set to come up when the system boots.

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

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

   Note: *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
   ```

   Note: *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. 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, ISIS servers, iNEWS servers, etc. This will not only test connection to the host server, but also verifies DNS.

   `ping –c 4 <hostname>`

3. Verify the same test, this time by pinging the host servers by IP address.

Note: *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 16.*

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>/<bitmask>;”
   ```

   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 associated with a bitmask and end with a semicolon. In the following example, a single IP address of 192.168.50.99 is added to the configuration:

   ```
   export ACS_SECURITY_FULL_TRUST_IPV4_MASK_LIST="127.0.0.1/25;192.168.50.99/32;"
   ```

   The /32 bitmask indicates that this is a single IP address. Also notice the required quotation marks that enclose the string. The 127.0.0.1/25 entry is a reference to the local MCS server.

***Note**: 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. In the following example, the single server at 192.168.50.99 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;192.168.50.99/32;192.16
   8.50.0/24;"
   ```

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

6. Restart the avid-acs-gateway service to enable the change:

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

7. If you are configuring multiple systems in a cluster, complete this process on all nodes.

Configure 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 (ISIS, Interplay Production, etc) is critical. Maintaining time synchronization between nodes in an MCS cluster configuration is particularly critical.

Setting the Time Zone

1. The installation script sets the default location to “America/New_York”. Verify this by viewing the contents of the Linux “clock” file.

   `cat /etc/sysconfig/clock`

   If the US/Eastern time zone is appropriate for your installation, skip this process. Otherwise, continue…

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. Example:

   `ls /usr/share/zoneinfo/US`

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

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).

   Note: *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.

Synching 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*.

***Note**: 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.*

***Note**: The use of the* iburst *option within the* cron *job is not recommended. It produces very rapid time shifts and can lead to synchronization problems.*

1. Verify the current date and time with the date command. Type: `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
   ```

   ***Note**: 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. Type: `service ntpd status`

   If the service is running, stop the service. Type: `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
   server 192.168.10.26
   ```

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 a line with the instructions for *cron*:

    ```
    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. Once again, verify the current date and time. It should be 10 minutes behind the correct time.

    ```
    date
    ```

13. 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
    ```

14. Verify the updated date and time:

    ```
    Date
    ```

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.

***Note**: 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**: Note 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:

      ```
      parted /dev/sdb
      ```

You will be presented with the Parted welcome screen and your user prompt will change from # to (parted).

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

```
mklabel gpt
```

c. You will be 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 will be returned to the (parted) prompt. Enter quit to exit the utility.

A final message will indicated that the /etc/fstab may 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 *one* 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 filesystem in the next step.

***Note**: 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
   ```

   Note in the above command you specify 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 filesystem 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
```

***Note**: If you receive an error indicating the mount point* /cache *does not exist, create the cache manually and issue the* mount *command again:*

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

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 .
    ```

    ***Note**: 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. Log in as *root* and edit the following file using a text editor (such as *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 close the file.

To re-enable 3G or Edge, edit the file and reset the “active” value to 1.

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
- ☐ Closed Captioning Service installer
- ☐ MAM Connector

For information on how to copy software to an MCS server, see **Copying Software to the MCS Server** on page 213.

Installing Security Updates

Once you have installed the operating system, please take a moment to resolve any outstanding RHEL security vulnerabilities. For information and links to KB articles with instructions, see the “Security Updates” section in the *Avid MediaCentral Platform Services ReadMe*.

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.

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 v2.7 installation process. The NEXIS Client is bundled with the MCS software for convenience and 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.

If required, instructions for **Downgrading the Avid Shared Storage Client** are provided in Appendix A of this document.

To upgrade the shared storage client:

1. Navigate to the location of the bundled shared storage client software:

   ```
   cd /opt/avid/Packages
   ```

2. 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
     ```

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 ISIS 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.

PART IV: CONFIGURING MCS

Chapter Overview

This chapter is divided into two main sections. Proceed to the section appropriate for your installation:

- Configuring MCS for MediaCentral UX and Media Composer Cloud
    - 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

The following table describes the topics covered in this chapter.

Step	Task	Time Est.
Configuring MCS for MediaCentral UX and Media Composer Cloud		
1	Updating the MediaCentral UX Configuration	2 min
	Covers use of the Configurator Tool.	
2	Logging into MediaCentral UX	5 min
	Log in to MediaCentral 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.	
7	Verifying the System Settings	
	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.	

Step	Task	Time Est.
11	Continuing the Installation	1 min
	Suggestions for additional steps to continue your installation.	

Step	Task	Time Est.
Configuring MCS for Interplay MAM		
1	Configuring MCS for Interplay MAM	5 min
	Introduction to MCS for MAM and prerequisites.	
2	Configuring the MediaCentral User Interface	5 min
	Verify the enabled components of the configurator.	
3	Creating the MAM System User	5 min
	Create the specialized user to be used with MediaCentral.	
4	Configuring the MCS Player	5 min
	Updating the Player Site Setting within MediaCentral UX.	
5	Enabling Remote Playback	10 min
	Description and process for enabling the alternate Remote Playback workflow.	
6	Continuing the Installation	1 min
	Suggestions for additional steps to continue your installation.	

Configuring MCS for MediaCentral UX and Media Composer Cloud

Now that you have installed and configured the operating system, you are ready to configure the software and settings specific to MediaCentral.

As a reminder, if you are running a cluster, complete this section on the master node only (unless instructed otherwise). Settings will be replicated to the other nodes during the cluster configuration process.

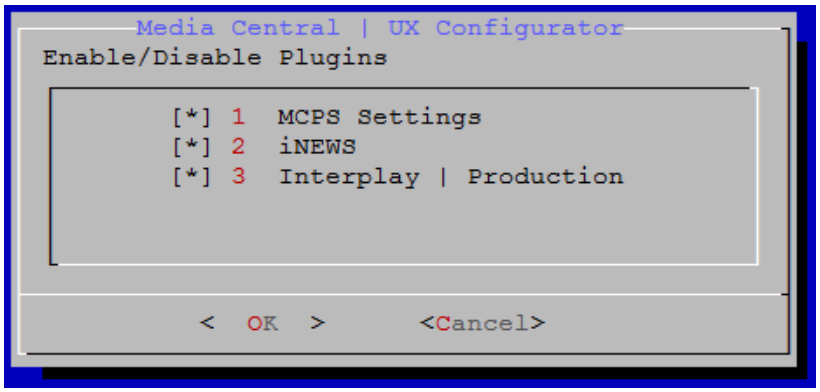
Updating the MediaCentral UX Configuration

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. 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, but 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.

1. Start the configurator by typing the following at the Linux prompt:

   ```
   /opt/avid/avid-interplay-central/configurator
   ```

   The configuration UI appears.



   ***Note**: Media Distribute (not shown) appears in the Configurator UI only if it has been installed on the system (through a separate installer).*

2. Select the appropriate application profile settings.

   The following table outlines typical settings by deployment type:

	MCPS Settings	iNEWS	Interplay Production	Media Distribute
MediaCentral & Media Distribute	ON	ON	ON	ON
Standard MediaCentral	ON	ON	ON	OFF
Interplay Production Only	ON	OFF	ON	OFF

	MCPS Settings	iNEWS	Interplay Production	Media Distribute
Media Composer Cloud	ON	OFF	ON	OFF
Interplay MAM	ON	OFF	OFF	OFF
iNEWS Only	OFF	ON	OFF	OFF

For example, for an iNEWS-only deployment without video playback, you would enable iNEWS and disable MCPS Settings and Interplay Production.

Note what each selection controls:

- **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.
- **Media Distribute**: Toggles the Interplay Media Distribute layout.

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.

   ***Note**: See **Working with the MediaCentral UX Configurator** for more information on the MediaCentral UX Configurator tool.*

Logging 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.

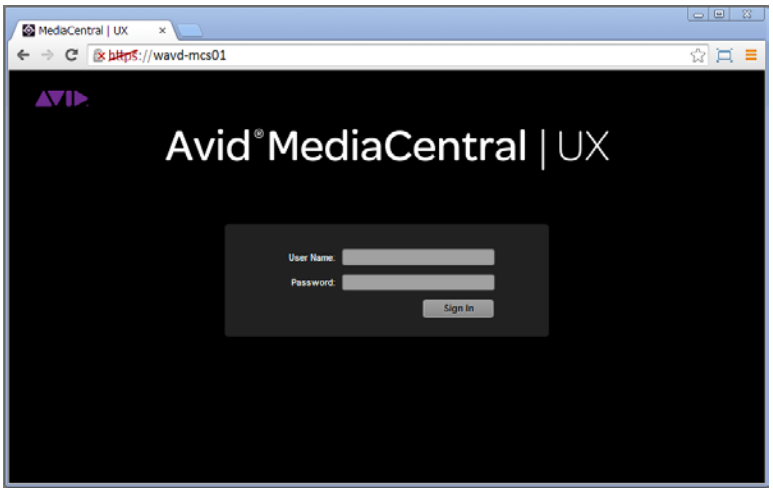
Note**: If you are configuring a cluster, you configure the MediaCentral UX System Settings once on the master node only. Do not configure these settings on slave or load balancing nodes. The other nodes inherit settings from the master through the clustering mechanisms. **Complete all remaining sections of this chapter on the Master node only.

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.

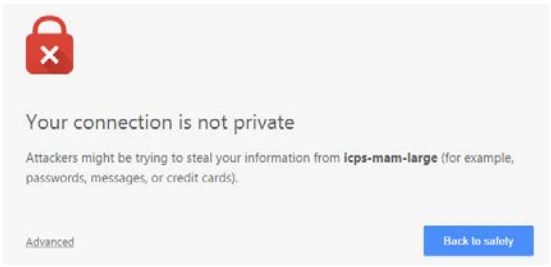
The MediaCentral UX sign-in screen appears.



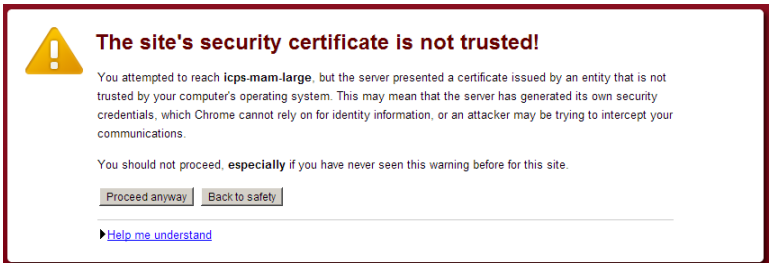
In place of the sign-in screen, you might see a warning indicating the connection is not private. The warning relates to SSL certificates.

For the purposes of installing and configuring MediaCentral UX, ignore the warning:

- Click **Advanced** and then the **Proceed to <*MediaCentral URL*> (unsafe)** link.



In older versions of Chrome (previous to release 37), the following warning is shown instead:



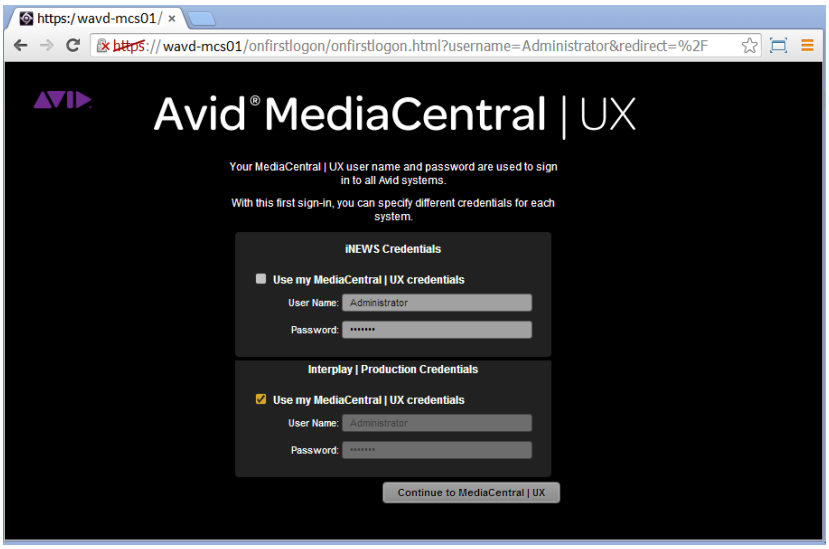
In the above case, click **Proceed Anyway**.

***Note**: 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).

   ***Note**: 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.*

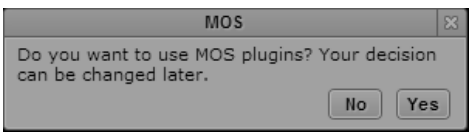
6. Click the "Continue to MediaCentral UX" button.

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. See **Modifying application.properties** for instructions.

   See the *Avid MediaCentral | UX User's Guide* for information on the Desktop Notifications feature.

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:



Selecting “Yes” will enable the “MOS enabled” checkbox in the user settings and prompt you to install the container needed for Active X controls.

Selecting “No” will not enable the MOS checkbox or prompt you to install any additional software. The MOS checkbox can be enabled manually in the user’s settings at any time.

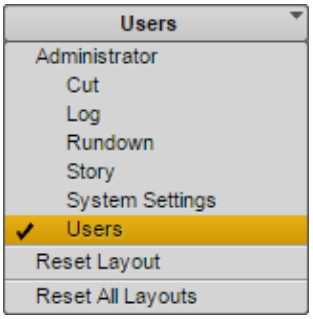
MOS plug-ins require additional software as described in “**Appendix F: Enabling MOS Active-X Plug-Ins** on page 272”.

***Note**: Active X controls and MOS plug-ins are not supported in the Safari browser or in Chrome v45 or higher. If you are running MCS v2.7 on Chrome 45 or later, you will not receive this dialog box. If you are running Chrome 44 or earlier, MOS options are still available.*

Changing the Administrator Password

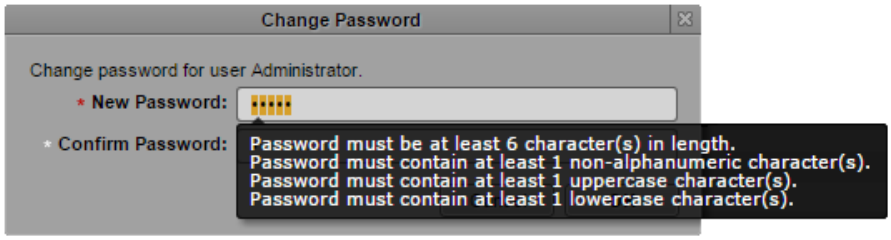
For security reasons, it is strongly suggested that you change the password for the *Administrator*

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.

***Note**: MediaCentral v2.1 introduced strong password enforcement. This feature was made optional in v2.2; however the default is to have strong passwords enabled. See the Avid MediaCentral | UX Administration Guide for more information on this feature and a process for “Turning Off Secure Password Requirements” if desired.*



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.

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 checkbox for "User must change password at next sign-in."
6. Click the Save button in the bottom-right corner of the window.

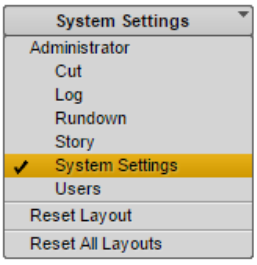
   The user account is created.

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*.

> ***Note**: 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.



Media Distribute settings are shown in the above example; however these settings will only appear if Media Distribute has been installed on the system. For more information see the *Media Distribute Installation and Configuration Guide*.

General Settings

This section configures general settings related to the overall operation of MediaCentral.

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 System ID is stored in the ACS bus. The System ID is displayed when you invoke the *ics_version* command from Linux or when you select Home>About within the MediaCentral user interface.

   ***Note**: 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 1.0 – 1.4 supported connection to only one iNEWS system. iNEWS Community support was added in ICS 1.5 with up to 24 members. ICS 1.8 increased possible community members to 50.

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 failover, 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. 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.

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 failover 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.

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.

   ***Note**: For instructions on retrieving archived messages, see the Avid MediaCentral | UX Administration Guide.*

3. Email Forwarding: If email forwarding is desired, enable the checkbox 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 checkbox if required by IT.
   f. Ignore TLS (Transport Layer Security): Select this checkbox 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" checkbox 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.

   ***Note**: 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 MedaCentral Playback Services (MCPS). MCPS is a set of services that run on the MCS servers that are responsible for the compression and playback of video and audio media.

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).

       ***Note**: MCS v2.5 and higher 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 ISIS through a Zone1 or Zone2 network connection, leave this box unchecked. If you are connecting through Zone3 (preferred configuration for ISIS 7500), enable this checkbox.

       ***Note**: For a refresher on ISIS Zone definitions, see **Network Interface Cards and Network Connections** on page 15.*

    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 ISIS. 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 ISIS. 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 ISIS.

   Options: 1GB Connection or 10GB Connection

5. Storage Locations. This section provides settings enabling MCS to connect to Avid ISIS 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 ISIS"

      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 ISIS. Every ISIS system has a virtual hostname, regardless of it being a single or failover configuration. **The Virtual Host Name must be entered in all lower-case**.

   e. User / Password: MediaCentral requires a dedicated user to access the ISIS storage system. Enter that user and password.

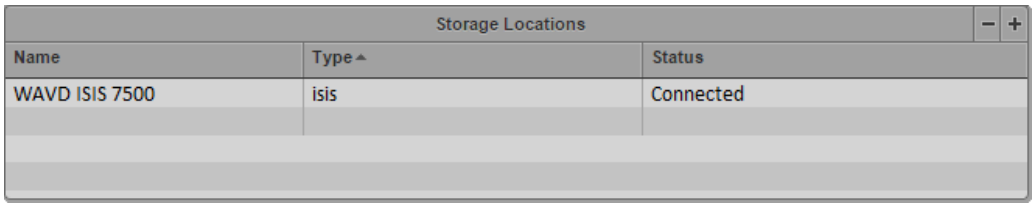
      Suggested User Name: MCSAdmin

      ***Note**: If you are connecting to multiple ISIS systems, ensure the same user/password is created on each ISIS.*

   f. System Directors: If you are connecting through Zone3 to ISIS, 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 ISIS connection.

6. Click Apply to save your changes. As the settings apply, MediaCentral will attempt to connect to the ISIS system(s) you have specified.



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.

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

   ***Note**: 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 ISIS user.

   ***Note**: 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.

   ***Note**: 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.

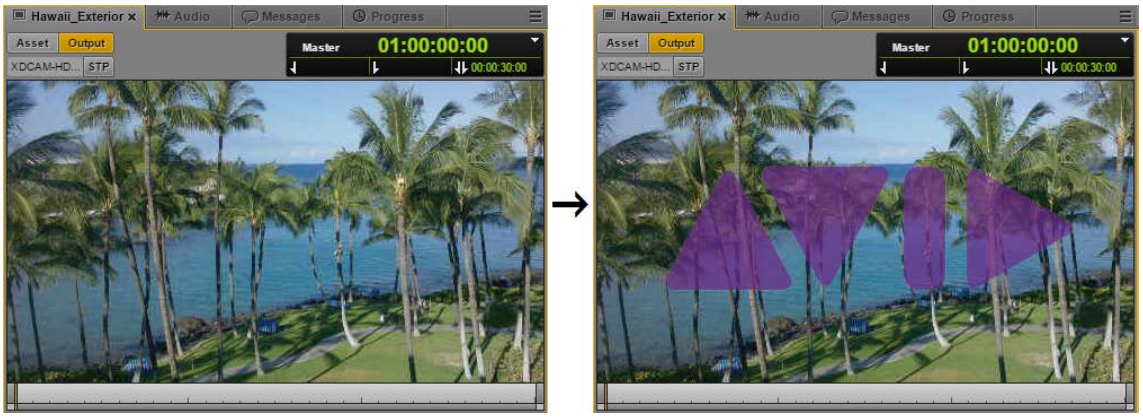
   For more information on these features, see the *MediaCentral UX Administration Guide*.

6. Click Apply to save your changes.

Enabling Asset Watermarking

MediaCentral Platform Services v2.7 introduces a Technology Preview of the Asset Watermarking feature for use with all MediaCentral 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.

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)

***Note**: Other file formats can introduce a negative impact on system performance. Unsupported file types result in a “Media Offline” message in the Media pane.*

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.

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 runs 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.

   ***Note**: 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=//vol1/Video_Uncompressed/
   matte/watermark.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.

   ***Note**: The START_IMAGE and END_IMAGE variables are for future use and must not be altered at this time.*

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
   ```

   ***Note**: 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`

   ***Note**: This step temporarily disconnects users from the playback service. Playback is briefly interrupted, but users are not logged out of the system.*
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

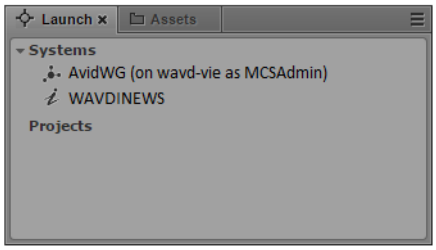
Now that you have configured the base system settings for connecting to iNEWS, Interplay Production and Avid ISIS (as applicable); perform some initial testing. If you are currently signed in to MediaCentral UX, sign out of MediaCentral and sign back in again prior to testing. This ensures the user has access to the updated System Settings.

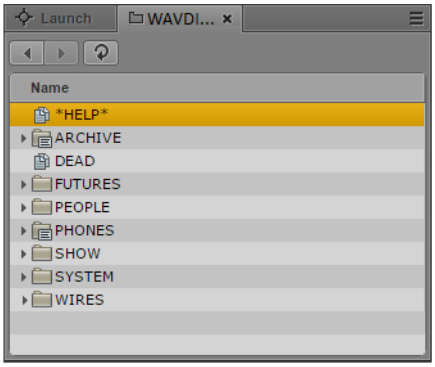
Verifying the iNEWS Connection

1. Select Log from the Layout menu in the top-right corner of the interface.

   ***Note**: 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**.*

   The Log layout will appear which consists of multiple default Panes. The Launch pane (shown on left) lists available iNEWS and Interplay Production workgroups.



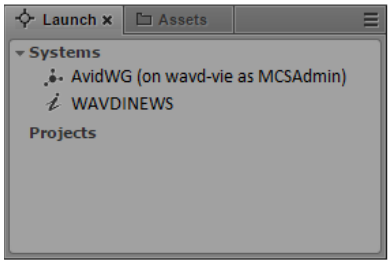


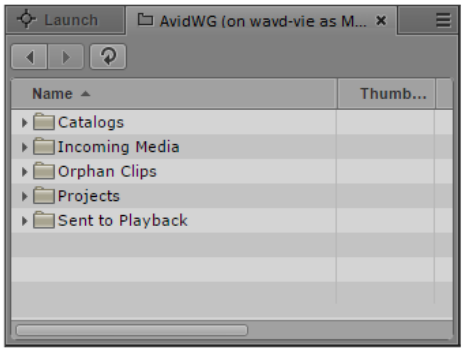
2. Double-click one of the iNEWS systems to verify the connection. If the connection is successful, a list of iNEWS assets should appear in the Assets Pane (shown on right).

Verifying the Interplay Production and ISIS 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.

1. In the Settings pane, select **Send to Playback**.

   When you open the STP settings, MediaCentral checks the configuration of the Interplay Administrator>Site Settings>Interplay Transfer Settings. If the Transfer Settings are populated with AirSpeed or Transfer Servers that are unavailable, the MediaCentral Send To Playback window will appear to be hung for a period of time. After a timeout period, the STP settings become available again. If you see a “Loading of Playback Device failed” (or similar) error, check the Transfer Settings configuration and verify that all AirSpeed and Transfer Servers are available.
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:

    i. 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.

    ii. When selecting a Transfer Engine, you will see the profiles configured on that server. Select an appropriate option for this profile.

e. Video Options:

    i. Long GOP: Select Long GOP if this profile will be used to transfer Long GOP media (XDCAM HD).

    ii. Accelerated STP: If you select both Long GOP and AirSpeed, the Accelerated STP option is activated. This option enables Play While Transfer (PWT).

    iii. AirSpeed: Select this option if transferring to an AirSpeed (classic), AirSpeed Multi Stream, or AirSpeed 5000.

    iv. 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.

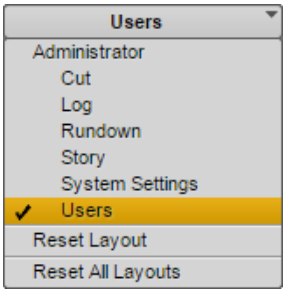
7. Once you have configured all required STP profiles, test your work by completing a Send To Playback test. See the *Avid MediaCentral | UX User's Guide* for information on creating a sequence within MediaCentral and sending media to playback.

Importing Domain Users

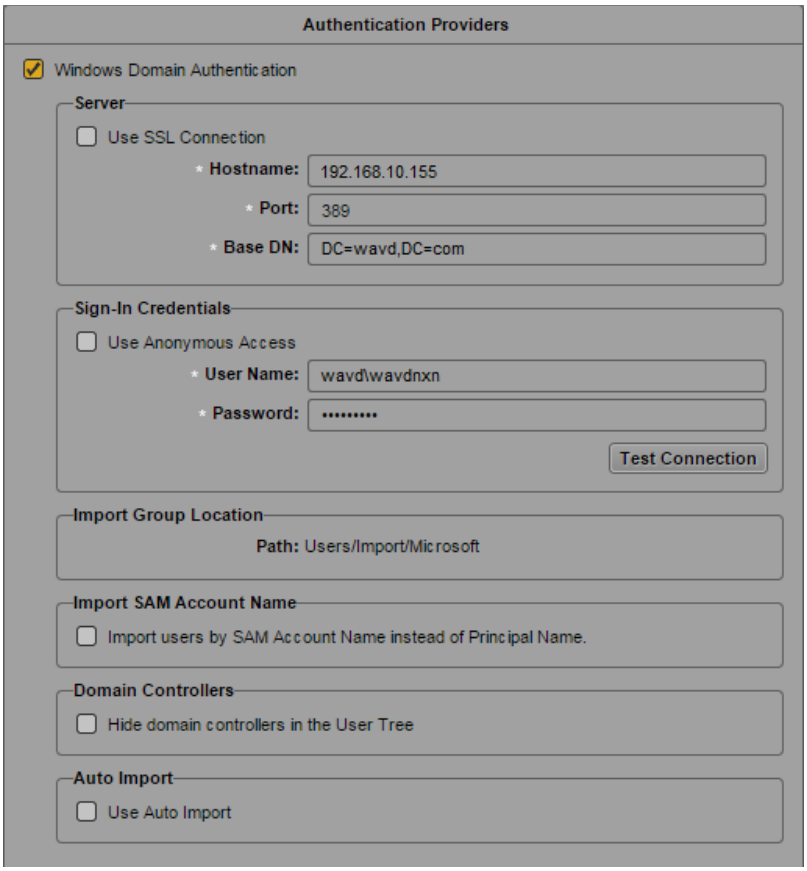
If your workflow includes signing into MediaCentral UX as a domain user, review the information below to configure settings and import domain users into MediaCentral.

See the *Avid MediaCentral | UX Administration Guide* for more information about any of these settings.

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. Enable the checkbox for “Windows Domain Authentication”.



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.

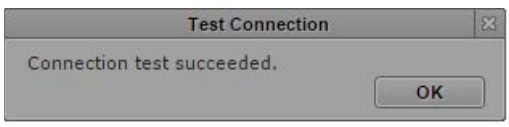
       How you type the Base DN depends on how your Active Directory is configured and which domains you want to authenticate from. If you want to authenticate from multiple sub-domains, set the common root of the sub-domains instead of the Base DN of a specific domain. Examples:

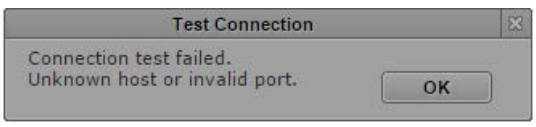
       DC=company,DC=com

       DC=company,DC=division,DC=com

       CN=Domain Users,OU=Organizational Unit, DC=company,DC=com
    e. Sign-In Credentials:
        i. If applicable, select "Use Anonymous Access". Selecting this will disable the user/password fields.
        ii. 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

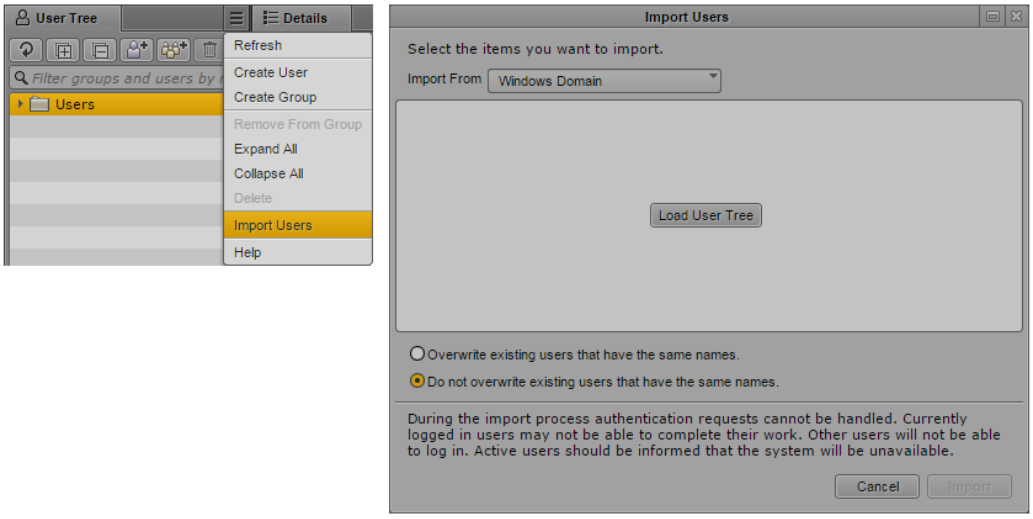
            Example: wavd\wavdnxn
    f. Import Group location: This is the location in the MediaCentral user tree where imported domain users will be located.
    g. Import SAM Account Name: (Optional) If your facility uses SAM Account Names instead of the newer Active Directory Principal Names, select "Import 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 checkbox 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.





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.



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.

    ***Note**: 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:

- **PART V: CLUSTERING**
- **PART VI: SHARDED MONGO**

  Part VI is required for all cluster and multi-zone configurations.

- **PART VII: VERIFYING THE INSTALLATION**

  Part VII must be completed for all installations.

- **PART VIII: INSTALLING THE CLOSED CAPTIONING SERVICE**
- **PART IX: INSTALLING CUSTOMIZABLE LOGGER**
- **PART X: INSTALLING THE MAM CONNECTOR**
- **PART XI: MULTI-ZONE CONFIGURATION**
- Media Distribute

  Refer to the *Media | Distribute Installation and Configuration Guide* for detailed installation instructions.

- Media Index

  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

For MCS to play Interplay MAM media, the filesystem containing the MAM proxies must be mounted on the MCS servers. The mounting is done at the operating system level using standard Linux commands for mounting volumes (e.g. *mount*). To automate the mounting of the MAM filesystem, create an entry in /etc/fstab.

> ***Note**: 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.

> ***Note**: Configuration must also take place on the Interplay MAM side, to set up permissions for MCS to access MAM storage, to point Interplay MAM to the MCS server or server cluster, etc. For instructions on this aspect of setup and configuration, please refer to the Interplay MAM documentation.*

> ***Note**: This step can be performed at any time during the installation.*

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.

See **Updating the MediaCentral UX Configuration** on page 93 for details on this process.

Creating the MAM System User

When integrating with Interplay MAM, a specialized user needs to be created within MediaCentral.

***Note**: If you are configuring an MCS cluster, complete this step on the Master Node only.*

1. With the MCS server up and running, log in to MediaCentral as the Administrator user.

   See **Logging into MediaCentral UX** on page 94 for details on this process.

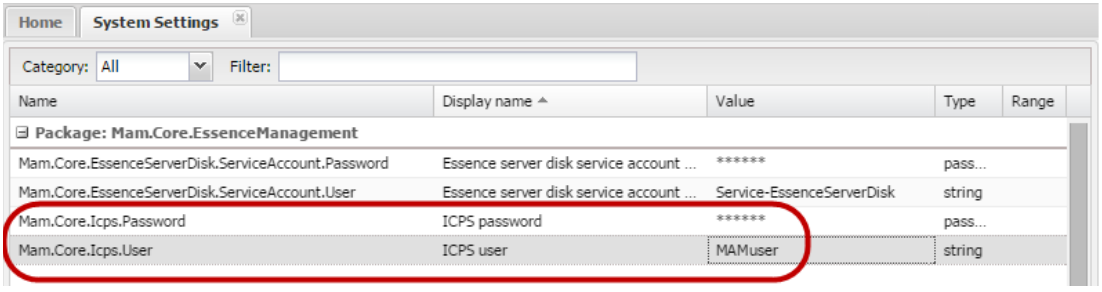
2. Select **Users** from the Layout selector.
3. Create a special role for the MAM user by clicking on the Create Role button in the Roles pane.
4. Click the Create Role button.
5. In the Details pane, type the properties for the new role:
   - Role name (e.g. **MAM**)
   - Advance License
   - Do not 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.

    The new MAM user is added to the User Tree, as a top-level user.

11. Ensure the System Settings on the Interplay MAM system are configured to make use of the assigned user name and password. Example:



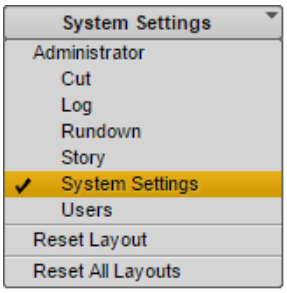
See the *Avid MediaCentral | UX Administration Guide* for more information about user creation and role assignment.

Configuring the MCS Player

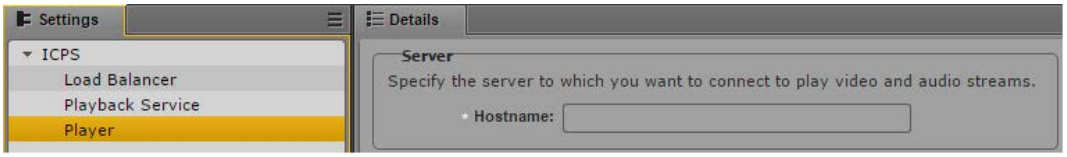
Configuring the MCS Player setting allows you to monitor connections to the player through the MediaCentral System Settings>MCPS>Load Balancer page.

***Note**: If you are configuring an MCS cluster, complete this step on the Master Node only.*

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 Server>Hostname field, enter the Fully Qualified Domain Name (FQDN) of the MCS server.



Example: wavd-mcs01.wavd.com

***Note**: 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 higher 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.

***Note**: 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:

- **PART V: CLUSTERING**
- **PART VI: SHARDED MONGO**

  Part VI is required for all cluster and multi-zone configurations.

- **PART VII: VERIFYING THE INSTALLATION**

  Part VII must be completed for all installations.

- **PART IX: INSTALLING CUSTOMIZABLE LOGGER**
- **PART X: INSTALLING THE MAM CONNECTOR**
- **PART XI: MULTI-ZONE CONFIGURATION**

PART V: 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 check for building the cluster.	
2	**Configuring the Player System Setting**	5 min
	Process for updating the MediaCentral Player System Setting.	
3	**Configuring DRBD**	10 min
	Initiate replication of the MCS PostgreSQL database.	
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**	15 min
	Connect all additional nodes to the cluster.	
6	**Replicating the File Caches using GlusterFS**	10 min
	Set up Gluster to mirror the caches, 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 second MCS server in the cluster is called the **Slave** node. In addition to load balancing and scale, it provides high-availability of some specialized MCS services. In the event of a failover, the Slave node becomes the new Master and owner of the MCS database. Additional nodes are known as "Load Balancing" nodes. These servers do not participate in high-availability; they provide load balancing and system scaling only.

Throughout this process the nodes will be identified by 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

The cluster is identified by the clients 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, but not including, Part IV 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).
- ☐ Virtual cluster hostname and a unicast IP address (used for communication between cluster and external systems – such as a MediaCentral UX client).
- ☐ A multicast IP address (used for internal communication between the cluster nodes). If necessary, a unicast IP can be used. However, specifying a unicast IP requires additional configuration.
- ☐ All hostnames and IP addresses, including the cluster's virtual name and IP, resolve normally through DNS.

Consult the Pre-Flight Checklist for a complete list of installation prerequisites.

http://avid.force.com/pkb/articles/en_US/readme/Avid-MediaCentral-Version-2-7-x-Documentation

For detailed information on MCS Clusters, see the *MediaCentral Platform Services Concepts and Clustering Guide* on the Avid Knowledge Base.

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.

1. Using Chrome or another qualified browser, log into MediaCentral as the Administrator user.
2. Select System Settings from the Layout pull-down menu.
3. In the Settings pane, select **MCPS> Player**.
4. Server: 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. Logout and exit the browser.

Configuring DRBD

In a clustered configuration, MCS uses the open source Distributed Replicated Block Device (DRBD) storage system software to replicate its 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.

> ***Note**: This procedure assumes a 20 GB partition exists on the RAID 1 mirrored system drive (**/dev/sda**). If you are installing MCS on supported HP or Dell hardware using the MCS Installation USB Drive, the required partition (**/dev/sda2**) was automatically created for you. If you are installing MCS on a server from another vendor, see **Installing MCS on Non-HP / Dell Hardware for Interplay MAM**.*

Explanation (do not type this example)

This procedure uses the *drbd_setup* command:

drbd_setup
[primary_host="<hostname>"] [secondary_host="<hostname>"]
{[primary_ip="<ip>"] [secondary_ip="<ip>"]}
{[primary_disk="<device>"] [secondary_disk="<device>"]}

where:

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).

***Note**: 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 /dev/sda2 values supplied by default will be sufficient.*

***Note**: The DRBD setup script is case-sensitive. The host names you enter must exactly match those defined for the master and non-master.*

1. On the Master node, change 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. 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.

3. Depending upon 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 receive error messages indicating the bus is not running and/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:

     ```
     Found some data
     ==> This might destroy existing data! <==

     Do you want to proceed?
     [need to type 'yes' to confirm]
     ```

     This indicates 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.

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, change 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  ]
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
128000 inodes, 511975 blocks
25598 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=524288000
16 block groups
32768 blocks per group, 32768 fragments per group
8000 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912

Writing inode tables:  0/16 1/16 2/16 3/16 4/16 5/16 6/16 7/16 8/16
9/1610/1611/1612/1613/1614/1615/16 done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 23 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
partition mounted at  /mnt/drbd
Starting postgresql-9.1 service: [  OK  ]
```

   ***Note**: A fail message might appear when the drbd_setup script tries to start PostgreSQL. This is normal.*

   Finally, information indicating 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 multicasting, see **Unicast Support in Clustering** for details on altering the configuration.

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), 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"
    ```

    ***Note**: 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".*

Explanation (do not type this example)

This procedure uses the *cluster setup-corosync* command:

```
cluster setup-corosync
[corosync-bind-iface =<interface>]
{[--corosync-mcast-addr="<ip>"]}
{[--rabbitmq_master="<device>"]}
```

where:

`--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 in this command.

`--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 in this command.

`--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 in this command.

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 rabbit 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="eth0" --admin_email="comma separated e-mail
list" --drbd_exclude="comma separated list of non-DRBD nodes"
```

Explanation (do not type this example)

This procedure uses the *cluster setup-cluster* command:

```
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>"}]
```

where:

--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.

***Note**: 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.

***Note**: Quotes are required in each of the above commands.*

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 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 monitoring 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.

***Note**: 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 – the fully configured MCS server – add the other servers to the cluster.

If your network does not support multicast activity, see **Unicast Support in Clustering** for details on altering the configuration.

1. On each of the non-master nodes in the cluster, complete one of the following:

   ***Note**: See the previous section for more information on each of the following commands.*

   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:

   ```
   bind_iface=eth0 bind_network=192.168.10.51 mcast_addr=239.192.1.1

   Shutting down UMS                                          [  OK  ]
   2012-11-19 15:48:57.891 -0500 - info: Done. System is up-to-date.
   generic – stop                                             [  OK  ]
   boot – stop                                                [  OK  ]
   Starting Corosync Cluster Engine (corosync):               [  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
   ```

***Note**: After this point, if you reconfigure any System Settings through the MediaCentral UI, 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.`

Replicating the File Caches using GlusterFS

When a playback request is sent to an MCS server, the media is obtained from ISIS (or Standard FS storage) and is quickly transcoded into an alternate delivery format. The transcoded media is stored in the system's "/cache" folder. 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. This is completed using GlusterFS, an open source software solution for creating shared file systems.

***Note**: 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 2.5 introduces a custom script which expedites the process for configuring Gluster across the cluster nodes.

***Note**: 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.

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
   ```

   Repeat this step 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 test that Gluster is replicating the caches correctly. This can completed by writing a file to one of the GlusterFS cache folders (e.g. */cache/download*) on one server and confirming that it appears on the other servers.

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/
   ```

PART VI: SHARDED MONGO

Chapter Overview

This chapter focuses on the creation of a sharded mongo configuration.

The following table describes the topics covered in this chapter:

Task
Sharded MongoDB 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

MediaCentral Platform Services v2.6 introduced a new Mongo database deployed in a "sharded" configuration. This new system enables authentication of both Avid and third party "plugins" or "applications" in MediaCentral through a collection of APIs called the Avid Connectivity Toolkit.

In an MCS cluster, the Corosync master and slave nodes each host a copy or "shard" of the Mongo database. Although the database is stored 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 configuration with remote nodes hosting shards of the other databases. This 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, an arbiter is still required. 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 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.

***Note**: Do not install the MongoDB arbiter on clustered Interplay Production Engines.*

For more information on this topic, see "MongoDB" in the *MediaCentral Platform Services Concepts and Clustering Guide*.

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**

If you plan to configure a multi-zone environment, complete the multi-zone configuration process prior to sharded Mongo. For details, see **PART XI: MULTI-ZONE CONFIGURATION**.

For additional information on sharded Mongo, see **Working with Sharded Mongo** in Appendix A.

Configuring Sharded Mongo for a Single Server

If you are configuring MediaCentral Platform Services on a single server, no additional steps are required. In a single server configuration, 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. Mongo depends heavily upon 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 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 on each cluster node.

    c. From the master node only, verify that the DNS server resolves all node host names correctly. Use the ping command to verify that each cluster node resolves correctly:

    `ping <node hostname>`

    Repeat the ping 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>`

2. From the master node, run the configuration file creation script:

    `/opt/avid/installer/ansible/mongo_setup`

    ***Note**: 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.*

    The script analyzes the current cluster configuration and prints its findings to the screen. This data is used by the final `setup.sh` script, found later in this process, to create the sharded Mongo environment. As seen in the following example, the results are only displayed at this time; no configuration files are created:

```
ZONE_NAME                                NODE_HOSTNAME       CLUSTER_ROLE
00000000-0000-0000-0000-000000000000     wavd-mcs01          master
00000000-0000-0000-0000-000000000000     wavd-mcs02          slave
00000000-0000-0000-0000-000000000000     wavd-mcs03          balance
```

Use the following information to verify that the configuration information is correct:

- ZONE_NAME = This is a unique identifier for the cluster zone. If you have a single zone, this value with be the same for all servers (00000000-0000-0000-0000-000000000000). If you have a multi-zone configuration, each zone will have its own ZONE_NAME. All servers within the zone share the same ID.
- 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.

***Note**: 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.*

3. 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:

   `/opt/avid/installer/ansible/mongo_setup -c`

4. The script updates the master "hosts" file which associates a node number with the short host name of each server that will participate in the sharded Mongo environment. Additionally, "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_setup 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 short host name. If the wrong nodes have been populated, 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 the load-balancing node. While the mongo_setup script might identify more than three servers, the hosts file will only list nodes that are part of the sharded Mongo configuration. If you have additional load-balancing nodes, these do not appear in the file.

5. Delete the default Mongo configuration on the Corosync master node:

   ```
   /opt/avid/installer/ansible/clean_sharded_mongo
   ```

   Repeat this step on the corosync slave node and all load-balancing nodes.

6. From the master node only, run the final setup script:

   ```
   /opt/avid/installer/ansible/setup.sh
   ```

   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.

Configuring Sharded Mongo with a (non-MCS) Linux 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 systems running either Red Hat Enterprise Linux (RHEL) v6.x or CentOS v6.x. 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 manually.

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 the all three systems.

   For detailed instructions, see **Verifying the *hosts* File Contents** on page 74.

2. Mongo depends heavily upon 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 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 on each cluster node and the arbiter.

c. From the master node only, verify that the DNS server resolves all node host names correctly. Use the ping command to verify that each cluster node resolves correctly:

```
ping <node hostname>
```

Repeat the ping 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>
```

3. Verify that the Linux arbiter is time synchronized with the cluster nodes.

For detailed instructions, see **Configure Date and Time Settings** on page 78.

4. On the arbiter, verify the contents of the `/etc/yum.repos.d/` directory:

```
ls /etc/yum.repos.d/
```

This directory should contain the base repo file "`rhel-source.repo`". If this file is not present, you must install "snappy" and "libselinux-python" from the RHEL CD. Snappy is required by Mongo and libselinux-python is required for the ansible scripts. Complete the following to install the required packages:

a. Create a mount point for the Linux installer CD:

```
mkdir /sysinstall
```

b. Load the Linux CD into the system's optical drive.

c. Mount the RHEL CD to the `/sysinstall` mount point:

```
mount /dev/cdrom /sysinstall
```

d. Install the required packages:

```
yum -c /sysinstall/media.repo install snappy
yum -c /sysinstall/media.repo install libselinux-python
```

5. On the arbiter, install the Mongo software using the yum package:

```
yum -c http://<host>:8085/mcs.repo install mongodb-org-server-mongod
mongodb-org-shell
```

Where <*host*> is the IP address of one of the MCS server nodes.

6. From the master node, run the configuration file creation script:

```
/opt/avid/installer/ansible/mongo_setup
```

***Note**: 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.*

The script analyzes the current cluster configuration and prints its findings to the screen. This data is used by the final `setup.sh` script, found later in this process, to create the

sharded Mongo environment. As seen in the following example, the results are only displayed at this time; no configuration files are created:

```
ZONE_NAME                                NODE_HOSTNAME       CLUSTER_ROLE
00000000-0000-0000-0000-000000000000     wavd-mcs01          master
00000000-0000-0000-0000-000000000000     wavd-mcs02          slave

================================================================
Warning!!! You have one region and 2 nodes. In this configuration
you need arbiter. Don't forget to add it manually.
================================================================
```

The script will display a message indicating that only 2 nodes are present in the cluster. This is an expected warning for a two node configuration. Continue with the remaining steps in the process to complete the arbiter configuration.

Use the following information to verify that the configuration information is correct:

- ZONE_NAME = This is a unique identifier for the cluster zone. If you have a single zone, this value with be the same for all servers (00000000-0000-0000-0000-000000000000). If you have a multi-zone configuration, each zone will have its own ZONE_NAME. All servers within the zone share the same ID.
- 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. In a two-node corosync cluster configuration, the script should not identify any additional systems.

***Note**: 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.*

7. 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:

   ```
   /opt/avid/installer/ansible/mongo_setup -c
   ```

   The script will again display a message indicating that only 2 nodes are present in the cluster. This is an expected warning for a two node configuration. Continue with the remaining steps in the process to complete the arbiter configuration.

   The script updates the master "`hosts`" file at `/opt/avid/installer/ansible` and a "node<#>" configuration file at `/opt/avid/installer/ansible/host_vars` (one for each Mongo node).

8. When configuring the arbiter on a non-MCS server, the mongo_setup script does not automatically populate the file with the arbiter data. This information must be added manually.

   a. On the master node, open the following file with the Linux *vi* editor:

      ```
      vi /opt/avid/installer/ansible/hosts
      ```

   b. Add the following line to the end of the configuration:

      ```
      node2 ansible_host=<arbiter_hostname>
      ```

      Where <*arbiter_hostname*> is the short host name of the arbiter.

The following is an example of the final output of the file:

```
#It's generated file from mongo_setup script

[shards]
shard0 shard_tag=region-0

[mcs_servers]
node0 ansible_host=wavd-mcs01
node1 ansible_host=wavd-mcs02
node2 ansible_host=wavd-mcsarbiter
```

The script adds nodes 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 the arbiter.

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

9. The mongo_setup script creates a "node<#>" file for each of the Mongo nodes. However, the arbiter node file must be created manually.

   a. The `/ansible/host_vars` directory should already contain two node files (node0 and node1) which represent the master and slave MCS servers.

      List the contents of this directory to verify that these files exist:

      ```
      ls /opt/avid/installer/ansible/host_vars
      ```

   b. Using the Linux vi editor, create a new node file for the arbiter on the master node:

      ```
      vi /opt/avid/installer/ansible/host_vars/node2
      ```

   c. Add the following information to the file:

      ```
      processes:
        - name: mongod
          shard: shard0
          service: iam
          mongod_port: 27100
          priority: 1
          master: false
          votes: 1
          arbiter: true

        - name: mongoc
          shard: config
          service: iam
          mongoc_port: 28001
          priority: 1
          master: false
          votes: 1
      ```

   ***Note**: If manual creation of the node file is tedious, the node1 file can be duplicated, renamed and modified to match the information above.*

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

10. Delete the default Mongo configuration on the corosync master node:

    ```
    /opt/avid/installer/ansible/clean_sharded_mongo
    ```

    Repeat this step on the corosync slave node and the Linux arbiter.

11. From the master node only, run the final setup script:

    ```
    /opt/avid/installer/ansible/setup.sh
    ```

    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.

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), Windows Server 2008 R2 (64 bit), 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.

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. Mongo depends heavily upon 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 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 on each cluster node and the arbiter.

   c. From the master node only, verify that the DNS server resolves all node host names correctly. Use the ping command to verify that each cluster node resolves correctly:

      ```
      ping <node hostname>
      ```

      Repeat the ping 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>
```

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. From the current Corosync master node, run the configuration file creation script:

   ```
   /opt/avid/installer/ansible/mongo_setup
   ```

   ***Note**: 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.*

   The script analyzes the current cluster configuration and prints its findings to the screen. This data is used by the final `setup.sh` script, found later in this process, to create the sharded Mongo environment. As seen in the following example, the results are only displayed at this time; no configuration files are created:

   ```
   ZONE_NAME                                NODE_HOSTNAME       CLUSTER_ROLE
   00000000-0000-0000-0000-000000000000     wavd-mcs01          master
   00000000-0000-0000-0000-000000000000     wavd-mcs02          slave
   ======================================================================
   Warning!!! You have one region and 2 nodes. In this configuration
   you need arbiter. Don't forget to add it manually.
   ======================================================================
   ```

   The script will display a message indicating that only 2 nodes are present in the cluster. This is an expected warning for a two node configuration. Continue with the remaining steps in the process to complete the arbiter configuration.

   Use the following information to verify that the configuration information is correct:

   - ZONE_NAME = This is a unique identifier for the cluster zone. If you have a single zone, this value with be the same for all servers (00000000-0000-0000-0000-000000000000). If you have a multi-zone configuration, each zone will have its own ZONE_NAME. All servers within the zone share the same ID.
   - 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. In a two-node corosync cluster configuration, the script should not identify any additional systems.

   ***Note**: 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:

   ```
   /opt/avid/installer/ansible/mongo_setup -c
   ```

The script will again display a message indicating that only 2 nodes are present in the cluster. This is an expected warning for a two node configuration. Continue with the remaining steps in the process to complete the arbiter configuration.

The script updates the master "hosts" file at `/opt/avid/installer/ansible` and a "node<#>" configuration file at `/opt/avid/installer/ansible/host_vars` (one for each Mongo node).

6. Delete the default Mongo configuration on the master node:

   ```
   /opt/avid/installer/ansible/clean_sharded_mongo
   ```

   Repeat this step on the corosync slave node.

7. From the master node only, run the final setup script:

   ```
   /opt/avid/installer/ansible/setup.sh
   ```

   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

   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.

8. Copy and unzip the MediaCentral_Services_<*version*>_Linux.zip installer package to the desktop of the Windows system that you plan to use as the Mongo arbiter.

9. If the Windows Firewall service is enabled, rules need to be added to the local system to ensure that the Mongo services can communicate without issue.

   a. On the Windows arbiter, 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 open Mongo specific ports:

      ```
      netsh advfirewall firewall add rule name="Mongo arbiter node"
      dir=in action=allow protocol=TCP localport=27100

      netsh advfirewall firewall add rule name="Mongo arbiter node"
      dir=out action=allow protocol=TCP localport=27100

      netsh advfirewall firewall add rule name="Mongo config node"
      dir=in action=allow protocol=TCP localport=28001

      netsh advfirewall firewall add rule name="Mongo config node"
      dir=out action=allow protocol=TCP localport=28001
      ```

10. Run the Mongo installer for Windows.

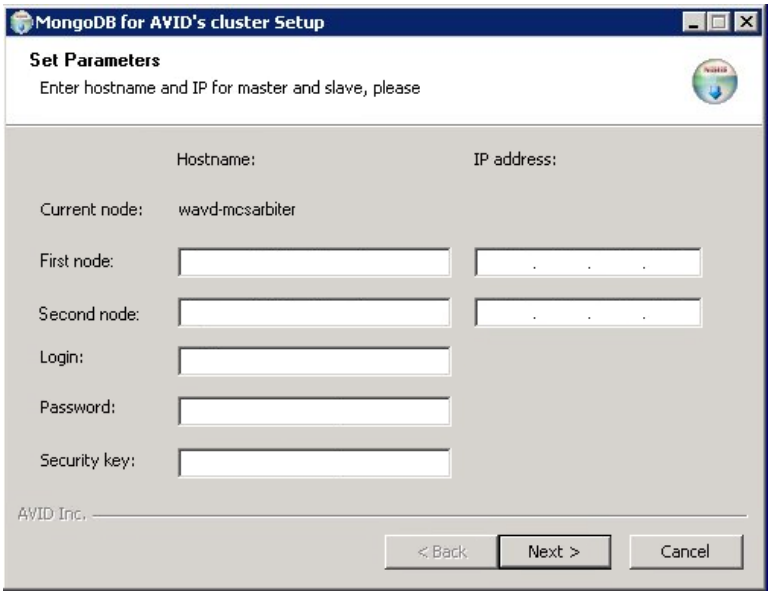
    a. On your Windows arbiter, navigate to the location of the installer.

    b. Double-click on setup-mongo-arbiter.exe to launch the installer application.

    c. Click Next at the Welcome screen.

d. Accept the default location for the installation and click Install.

e. Configure the following in the Set Parameters window:



- First node: Enter the short host name and IP address of the current Corosync master node.
- Second node: Enter the short host name and IP address of the current Corosync slave node.
- Login: Enter the default Mongo user login: admin
- Password: Enter the default Mongo user password: AvidAdmin_123!
- Security key: Enter the contents of the "secret" file located on the master node:

  `/var/lib/mongod-iam-shard0-27100/secret`

  Example: C450B913A1A5344F

f. Click Next.

The installer adds the Corosync master and slave nodes to the local Windows hosts file (\Windows\System32\drivers\etc) and verifies that the Mongo nodes can be reached.

If the Mongo nodes are not found or if the Login, Password or Security keys are incorrect, the following error is displayed:

"Can't add arbiter. Check login, password or IP of nodes."

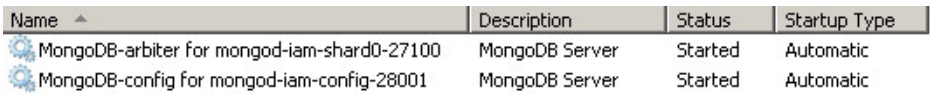
Check the information entered into the installer and click Next to try again.

***Note**: The Mongo Password is stored on the primary node at: `/opt/avid/installer/ansible/group_vars/all`. The password can be customized, but this must be completed **before** running the setup.sh script on the primary node.*

g. Click Finish to complete the installation.

The completed installation will result in the following:

- Application folder at: C:\mongodb
- A new application, listed as "MongoDB 3.2.4 (64 bit)" in the Programs and Features Control Panel
- Two new services:



11. Once installed, the Mongo installer can be deleted from the Windows desktop.

If needed, see **Working with Sharded Mongo** in Appendix A for the steps involved in uninstalling the Windows arbiter.

Configuring Sharded Mongo in a Multi-Zone Configuration

Multi-zone deployments are similar to local cluster deployments in that multiple nodes participate in the sharding process. The primary difference is the potential number of shards involved.

Arbiters are not required for multi-zone configurations. If your master zone consists of a 2-node Corosync cluster, MCS server(s) in the slave zone provide the tie-breaking vote in an election. This eliminates the need for a dedicated arbiter.

MediaCentral v2.7 supports multi-zone configurations consisting of mixed v2.5.x – v2.7 zones. Only zones that are running MCS v2.6 or higher can be included in the sharded Mongo configuration. Zones running older versions of software will continue to function as normal, but will not benefit from the enhanced sharded Mongo functionality.

Complete the following steps to create a multi-zone Mongo installation. The "master node" in this process refers to the master node of the master zone.

Warning! Prior to completing this process, you must have a functional multi-zone configuration. For more information, see PART XI: MULTI-ZONE CONFIGURATION on page 194.

***Note**: If you are creating a new multi-zone configuration and your environment consists of an MCS v2.6 or higher 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 from Linux or Windows, see **Working with Sharded Mongo** in Appendix A.*

To configure sharded Mongo:

1. Update the hosts file on all shards 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. Mongo depends heavily upon 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 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 on each server in the multi-zone configuration.

    c. From the master node only, verify that the DNS server resolves all node host names correctly. Use the ping command to verify that each cluster node resolves correctly:

    `ping <node hostname>`

    Repeat the ping 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 the pingable_ip can be located on the network for any zone that consists of a cluster:

    `ping <IP address>`

3. Verify that all nodes are time synchronized.

    For detailed instructions, see **Configure Date and Time Settings** on page 78.

4. From the master node of the master zone, view the current configuration by running the following script:

    `/opt/avid/installer/ansible/mongo_setup`

    ***Note**: 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.*

    The script analyzes the current configuration of each zone and prints its findings to the screen. This data is used by the final `setup.sh` script, found later in this process, to create the sharded Mongo environment. As seen in the following example, the results are only displayed at this time; no configuration files are created:

```
ZONE_NAME                              NODE_HOSTNAME       CLUSTER_ROLE
df613e50-074c-4aad-a8c3-8c21225503bc   wavd-mcs01          master
df613e50-074c-4aad-a8c3-8c21225503bc   wavd-mcs02          slave
df613e50-074c-4aad-a8c3-8c21225503bc   wavd-mcs03          balance
612a0570-a694-4141-a5fb-5abc36f15d6d   news-mcs            master
54a3b6cb-7267-43bf-95e7-480cf27305c3   nyc-mcs             master
```

Use the following information to verify that the configuration information is correct:

- ZONE_NAME = This is a unique identifier for the cluster zone. If you have a single zone, this value with be the same for all servers (00000000-0000-0000-0000-000000000000). If you have a multi-zone configuration, each zone will have its own ZONE_NAME. All servers within the zone share the same ID.
- 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).

***Note**: 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 other two zones are single server configurations.

***Note**: The mongo_setup script might identify additional servers that will not participate in the sharded Mongo configuration. In comparison, the "hosts" configuration file modified in the following step only lists nodes that host a Mongo shard.*

If the information is not correct, troubleshoot the issue before continuing.

5. 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:

   ```
   /opt/avid/installer/ansible/mongo_setup -c
   ```

6. The script updates the master "hosts" file which associates a node number with the short host name of each server that will participate in the sharded Mongo environment. Additionally, "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_setup script

   [shards]
   shard0 shard_tag=region-0

   [mcs_servers]
   node0 ansible_host=wavd-mcs01
   node1 ansible_host=wavd-mcs02
   node2 ansible_host=news-mcs
   node3 ansible_host=nyc-mcs
   ```

   Verify that each node is created with the short host name. If the wrong nodes have been populated, resolve the situation and run the script again.

***Note**: Verifying the hosts file is especially important for complex configurations as the script might populate the file with incorrect or non-optimal information.*

7. Delete the default Mongo configuration on the master node of the master zone:

   ```
   /opt/avid/installer/ansible/clean_sharded_mongo
   ```

   Repeat this step on all other nodes in all zones that will take part in the sharded Mongo configuration.

8. From the master node only, run the final setup script:

   ```
   /opt/avid/installer/ansible/setup.sh
   ```

   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=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.

Adding a Zone to a Sharded Mongo Multi-Zone Environment

Only servers that are running MCS v2.6 or higher can be included in the sharded Mongo configuration. 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 **PART XI: MULTI-ZONE CONFIGURATION** on page 194.
3. Update the hosts file on all shards in all zones with the IP address, hostname and FQDN of any node that will be joining the sharded Mongo configuration.

   For detailed instructions, see **Verifying the *hosts* File Contents** on page 74.

4. Mongo depends heavily upon correct hostname resolution. Before configuring Mongo, verify that all hostnames return the expected values. Complete the following:

   a. Use the hostname command to verify the short host name of the node:

      ```
      hostname
      ```

      Repeat this command on each server being added to 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 on each server being added to the multi-zone configuration.

c. From the any, verify that the DNS server resolves all node host names correctly. Use the ping command to verify that each cluster node resolves correctly:

```
ping <node hostname>
```

Repeat the ping command for each server being added to the multi-zone configuration, verifying that each node returns the correct information from DNS.

5. Verify that all nodes are time synchronized.

For detailed instructions, see **Configure Date and Time Settings** on page 78.

6. Prior to making any changes to the configuration, review of the current ansible hosts file:

```
cat /opt/avid/installer/ansible/hosts
```

The following is an example of the file output:

```
#It's generated file from mongo_setup script

[shards]
shard0 shard_tag=region-0

[mcs_servers]
node0 ansible_host=wavd-mcs01
node1 ansible_host=wavd-mcs02
node2 ansible_host=news-mcs
node3 ansible_host=nyc-mcs
```

Take note of the current node order. When adding the new zone, it is very important that the new node or nodes are added to the end of the `mcs_servers` list.

7. From the master node of the master zone, view the current configuration by running the following script:

```
/opt/avid/installer/ansible/mongo_setup
```

***Note**: 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.*

The script analyzes the current configuration of each zone and prints its findings to the screen. This data is used by the final `setup.sh` script, found later in this process, to create the sharded Mongo environment. As seen in the following example, the results are only displayed at this time; no configuration files are created:

```
ZONE_NAME                               NODE_HOSTNAME       CLUSTER_ROLE
df613e50-074c-4aad-a8c3-8c21225503bc    wavd-mcs01          master
df613e50-074c-4aad-a8c3-8c21225503bc    wavd-mcs02          slave
df613e50-074c-4aad-a8c3-8c21225503bc    wavd-mcs03          balance
612a0570-a694-4141-a5fb-5abc36f15d6d    news-mcs            master
```

```
54a3b6cb-7267-43bf-95e7-480cf27305c3    nyc-mcs             master
777fh6a0-8456-22jk-76z2-512cvb7992ii    mynew-mcs           master
```

Use the following information to verify that the configuration information is correct:

- ZONE_NAME = This is a unique identifier for the cluster zone. If you have a single zone, this value with be the same for all servers (00000000-0000-0000-0000-000000000000). If you have a multi-zone configuration, each zone will have its own ZONE_NAME. All servers within the zone share the same ID.
- 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).

***Note**: 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 thee zones are single server configurations.

Verify that the server or servers from the newly added zone appear in the output.

***Note**: The mongo_setup script might identify additional servers that will not participate in the sharded Mongo configuration. In comparison, the "hosts" configuration file modified in the following step only lists nodes that host a Mongo shard.*

If the information is not correct, troubleshoot the issue before continuing.

8. 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:

   ```
   /opt/avid/installer/ansible/mongo_setup -c
   ```

9. The script updates the master "hosts" file which associates a node number with the short host name of each server that will participate in the sharded Mongo environment. Additionally, "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_setup script

   [shards]
   shard0 shard_tag=region-0

   [mcs_servers]
   node0 ansible_host=wavd-mcs01
   node1 ansible_host=wavd-mcs02
   node2 ansible_host=news-mcs
   node3 ansible_host=nyc-mcs
   node4 ansible_host=mynew-mcs
   ```

Verify that the node or nodes in the new zone have been added to the end of the list. In the example above, “mynew-mcs” has been added as node4. If the new nodes are added to the middle of the node list, the sharded Mongo configuration will fail. Also verify that each node is created with the short host name. If the wrong nodes have been populated, resolve the situation and run the script again.

***Note**: Verifying the hosts file is especially important for complex configurations as the script might populate the file with incorrect or non-optimal information.*

10. Delete the default Mongo configuration on any server being added to the multi-zone configuration:

    ```
    /opt/avid/installer/ansible/clean_sharded_mongo
    ```

    Repeat this step on each new server node. **DO NOT** run the clean command on any server that is already configured for sharded Mongo.

11. From the master node only, run the final setup script:

    ```
    /opt/avid/installer/ansible/setup.sh
    ```

    The script will create a new shard with the proper shard tag, add new shard replicas to all existing nodes, run avid-iam-migration in "add region mode", and deploy the avid-iam service on new node(s). All existing shards are unaltered by this process.

    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=93  changed=21  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.

PART VII: VERIFYING THE INSTALLATION

Chapter Overview

This chapter focuses on testing and verification of the completed installation.

The following table describes the topics covered in this chapter:

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 Failover	varies
	For configurations with a cluster, verifying failover 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 the MCS System Settings and the MCS 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 log into MediaCentral? Can they play media?
- Can mobile clients log into MediaCentral? Can they play media?
- Can Media Composer Cloud clients log into MediaCentral. Can they play media?
- Can you access and search the Interplay Production database?
- Can you access and search the iNEWS database?
- Can you create a sequence and Send To Playback?

  ***Note**: Send To Playback is an excellent test as it simultaneously verifies connection to ISIS, Interplay Production, MediaCentral Distribution Service, Interplay Production Services Engine, Interplay Transcode and potentially Interplay STP Encode and Interplay Transfer Engine.*
- Can you Delivery media to a remote workgroup? Can you "Deliver To Me"?
- Can Media Composer Cloud clients upload/download media?
- Does the Messaging Pane deliver messages between MediaCentral Users? Does it deliver messages between MediaCentral and Media Composer?
- Do Media Index searches return expected results?
- For Multi-Zone configurations, can you log in to MediaCentral from a Slave zone? This tests the accessibility of the user database on the Master Zone.

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 node, for failovers). 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
   ```

2. The system should respond with the following:

   ```
   master (pid XXXX) is running...
   ```

3. If the service is not running:

   a. Check the *postfix* service run-level configuration:

   ```
   chkconfig –-list postfix
   ```

   The configuration returned should look like this (run levels 2–5 *on*):

   ```
   postfix 0:off 1:off 2:on 3:on 4:on 5:on 6:off
   ```

   b. To enable run levels 2–5, type the following:

   ```
   chkconfig postfix on
   ```

   c. Start the service:

   ```
   service postfix start
   ```

4. 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 **Return**:

   The system responds by moving the cursor into the body of the email.

   Type a line or two of text, as desired.

   Note: *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.

Testing Cluster Failover

If your configuration consists of a cluster, verifying the system's ability to failover 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`" asks the tool to display the status of the cluster with fail-counts. Each time that a service fails, a node failure count is retained by the system. Except for the AvidAll service, the default threshold for failures of each service is two (2). Before testing the cluster, you will want to clear the fail-counts. If you do not, the cluster will failover automatically, and perhaps unexpectedly, when the threshold is reached.

To test cluster failover:

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 configured
31 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 ]
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:
```

Note the line identifying the Master node:

- AvidClusterIP

Note that the Master node always runs the following services:

- AvidIPC (avid-interplay-central)
- AvidUMS (avid-ums)
- AvidUSS (avid-uss)
- AvidACS (avid-acs-ctrl-core)

In the above list, the actual service name, as it would appear at the Linux command line, is shown in parentheses. Additional services may appear in the monitoring utility depending upon your installation.

***Note**: 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 failure 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
```

***Note**: Make sure your SSH window is large enough (vertically) to see the failure counts.*

4. If failures exist, they need to be cleared before testing the failover:

```
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.

***Note**: 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). For example, for the **AvidAll** resource, use **AvidAllEverywhere**. For **AvidConnectivityMon**, use **AvidConnectivityMonEverywhere**.*

***Note**: You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.*

For example, to reset the fail-count for AvidALL resource, issue the following command:

```
crm resource cleanup AvidAllEverywhere
```

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 failover 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.

   ***Note**: During the failover process, any active MediaCentral clients will receive a message indicating the need to log back in. Playback might be briefly affected.*

9. If failure 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, 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 failure counts were added to the monitoring tool, clear them with the `crm resource cleanup` command.
13. Repeat the process to test failover in the opposite direction. Remember to clear any failure counts at the end of the process and verify basic functionality.

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.

To verify the RabbitMQ service status:

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"},
```

Review the output of the command and verify there are no obvious error messages such as "service is dead but pid (*xxxxx*) is running".

Repeat the command on all cluster nodes.

To verify that RabbitMQ cluster status:

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.
```

If you do not see similar results or need additional information on RabbitMQ, including troubleshooting assistance, see:
http://avid.force.com/pkb/articles/en_US/troubleshooting/RabbitMQ-cluster-troubleshooting

More information on Corosync and RabbitMQ clustering can be found in the *MediaCentral Platform Services Concepts and Clustering Guide*.

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:

Query the ACS bus database using the *acs-query* command with using the *--path* option:

```
acs-query --path=serviceType
```

Output similar to the following ought to be presented:

```
"avid.acs.registy"
```

The above output indicates RabbitMQ, MongoDB and PostgreSQL are all running and reachable by the ACS bus (since no errors are present). It also indicates the "avid.acs.registry" bus service is available.

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 will be accessed from the MediaCentral 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.

***Note**: Currently, connecting to MediaCentral 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 from outside the corporate firewall through NAT, this domain name must resolve to an external (public) IP address.

***Note**: 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.

   ***Note**: Refreshing the web page may return a different node name. This is normal.*

If the output does not match, you may be able to log into MediaCentral on a remote client, but playback may 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** for instructions.

> ***Note**: 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 the MCS System Settings and the MCS 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.

> ***Note**: 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 backing up multiple nodes in a cluster, 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

Directory/File	Description
/etc/resolv.conf	DNS 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 higher.
/opt/avid/etc/avid/avid-interplay-central/config/application.properties	Contains customized options for MCS.
/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. ***

***Note**: 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. For the default root user password, contact your Avid representative.*

To back up the system settings and MCS database:

***Note**: 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.*

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 214.

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
   ```

   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
   ```

   ***Note**: Note 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.

   ***Note**: 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 214.

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 214.

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.

   > ***Note**: 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.
   ```

   > ***Note**: 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 214.

8. If you have a cluster, repeat the process on each node.

PART VIII: INSTALLING THE 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	Installing the Closed Captioning Service on a Single Server	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 in the United States and Canada 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 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.

***Note**: The Closed Captioning Service installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and log off during the installation or upgrade procedures.*

***Note**: Ensure that the "Virtual Host Name" configured within the Playback Service Settings 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>"

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.

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** and **Copying Software to the MCS Server** 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. If necessary, unpack the package containing the CC Service installations files:

   ```
   tar -xzvf MediaCentral_ClosedCaptioning_Service_<x.x.x>.tar.gz
   ```
5. Navigate to the newly created directory:

   ```
   cd MediaCentral_ClosedCaptioning_Service_<x.x.x>_<build>_Linux
   ```

Installing the Closed Captioning Service on a Single Server

1. If you have not already done so, navigate to the directory containing the CC Service installation script, `install.sh`:

   ```
   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 failover.

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**

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 failover. 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 failover, make sure to follow the order represented below.

To take the cluster offline:

1. Begin taking the cluster off-line 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.

1. If you have not already done so, navigate to the directory containing the CC Service installation script, `install.sh`:

   ```
   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!
   Cluster detected
   avid-ccc is not running                                    [  OK  ]
   avid-ccc is not running                                    [  OK  ]
   [INFO] chkconfig avid-ccc off
   Cleaning up AvidCCC on wavd-mcs01
   Cleaning up AvidCCC on wavd-mcs02
   Cleaning up AvidCCC on wavd-mcs03
   Waiting for 3 replies from the CRMd.. OK
   ```

   ***Note**: When installing the service on additional nodes, you will see one additional informational message:*

   ```
   [INFO] Already configured, service has been stopped and disabled
   ```

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
   ```

Bringing the Cluster Online

With the Closed Captioning Service installed on all nodes, bring the cluster back online. Make sure to follow the order represented below.

To bring the cluster online:

1. Frist, 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

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.
   - Verify the fail-counts for the following resources (at a minimum): AvidCCC, AvidIPC, AvidUMS, AvidACS, pgsqlDB.

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

   ***Note**: 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). For example, for the AvidAll resource, use AvidAllEverywhere. For AvidConnectivityMon, use AvidConnectivityMonEverywhere.*

   ***Note**: You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.*

   For example, to reset the fail-count for AvidALL resource, issue the following command:

   ```
   crm resource cleanup AvidAllEverywhere
   ```

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 170.

2. Take the cluster offline.

   For details, see **Taking the Cluster Offline** on page 171.

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.

   ***Note**: 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 172.

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.

- Verify the fail-counts for the following resources (at a minimum): AvidIPC, AvidUMS, AvidACS, pgsqlDB.

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

   ***Note**: 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). For example, for the AvidAll resource, use AvidAllEverywhere. For AvidConnectivityMon, use AvidConnectivityMonEverywhere.*

   ***Note**: You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.*

   For example, to reset the fail-count for AvidALL resource, issue the following command:

   ```
   crm resource cleanup AvidAllEverywhere
   ```

PART IX: INSTALLING 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	15 min
	Covers the areas where administrators can verify the installation.	
- -	Uninstalling the Customizable Logger	5 min
	Process for removing the Customizable Logger software from the MediaCentral server.	
- -	Working with the Customizable Logger	- -
	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 MediaCentral servers in a non-sharded MongoDB database.

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.

***Note**: The Customizable Logger installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and log 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** and **Copying Software to the MCS Server** 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>_Linux.zip`
4. If necessary, unpack the package containing the installations files:

   `tar -xzvf MediaCentral_Customizable_Logger_<x.x>_<build>_Linux.tar.gz`
5. Navigate to the newly created directory:

   `cd MediaCentral_Customizable_Logger_<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, `install.sh`:

   `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 180 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.

***Note**: 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.

1. If you have not already done so, navigate to the directory containing the installation script, `install.sh`:

   `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!
   ```

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=AvidIPCmeta_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

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

   ***Note**: 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:

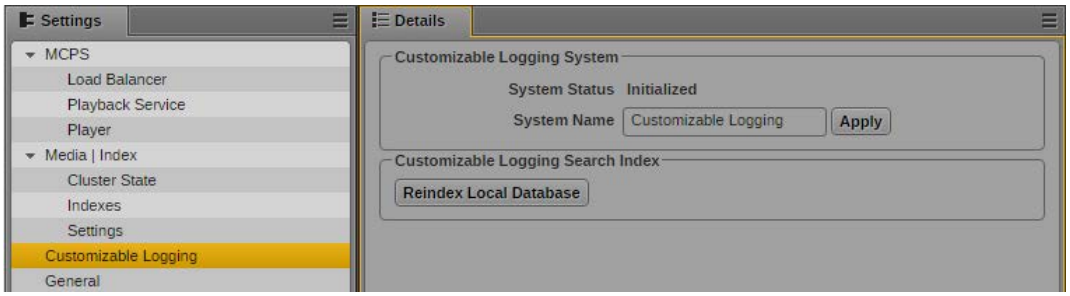
   ```
   crm resource cleanup AvidAllEverywhere
   ```

***Note**: 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** to update the System Name associated with the logging index.

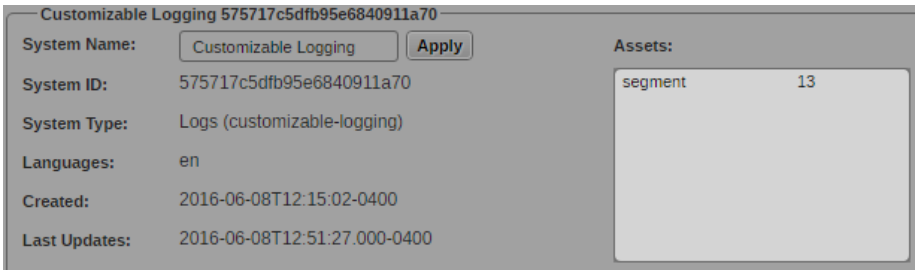
Configuring the Customizable Logger

The installation of the Customizable Logger adds a new line item to the MediaCentral UX System Settings called “Customizable Logging”.



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:



***Note**: 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.

***Note**: The System Name will appear in the two above locations only after the first time that the Customizable Logger is used to create searchable data.*

To customize the System Settings:

1. Using Chrome or another qualified browser, log 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 Logging Controls.
4. Enter a customized System Name in the text box and click Apply.

   Examples: <*hostname*>-Logger or NewYork-Logger

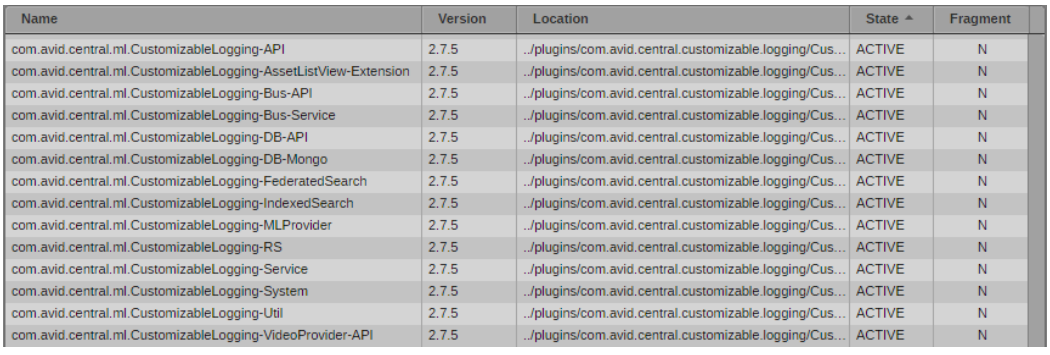
Verifying the Installation

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.

***Note**: The logging index will appear after the first time the Customizable Logger is used to create searchable data.*

To verify the installation:

1. Using Chrome or another qualified browser, log 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.



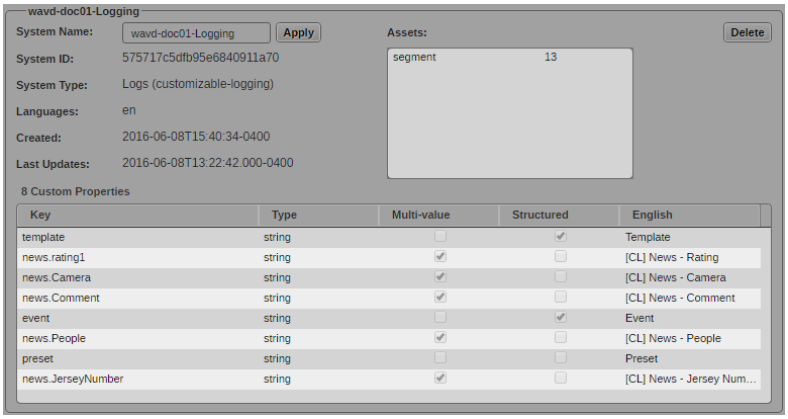
Name	Version	Location	State	Fragment
com.avid.central.ml.CustomizableLogging-API	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-AssetListView-Extension	2.7.5	../plugins/com.avid.central.customizable.logging/Cus...	ACTIVE	N
com.avid.central.ml.CustomizableLogging-Bus-API	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

All modules must show a status of ACTIVE in the State column.

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, log 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 Media | Index > Indexes.
4. Verify that Details pane shows a new index for the Customizable Logger.



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.

Uninstalling the Customizable Logger

In the event that you need to disable functionality added by the Customizable Logger, use one or more of 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.

To uninstall the Customizable Logger 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 "To remove the logging index" to reset the index data.

To uninstall the Customizable Logger on a cluster:

1. Verify the current Master, Slave and load balancing nodes.
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.
   - Verify the fail-counts for the following resources (at a minimum): AvidIPC, AvidUMS, AvidACS, pgsqlDB.
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

   ***Note**: 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). For example, for the AvidAll resource, use AvidAllEverywhere. For AvidConnectivityMon, use AvidConnectivityMonEverywhere.*

   ***Note**: You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.*

   For example, to reset the fail-count for AvidALL resource, issue the following command:

   `crm resource cleanup AvidAllEverywhere`
7. If desired, proceed to "To remove the logging index" to reset the index data.

To remove 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.

1. Using Chrome or another qualified browser, log 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 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 "To reset the MongoDB database" to remove all logging data from the system.

To reset the MongoDB database:

***Warning**: 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.

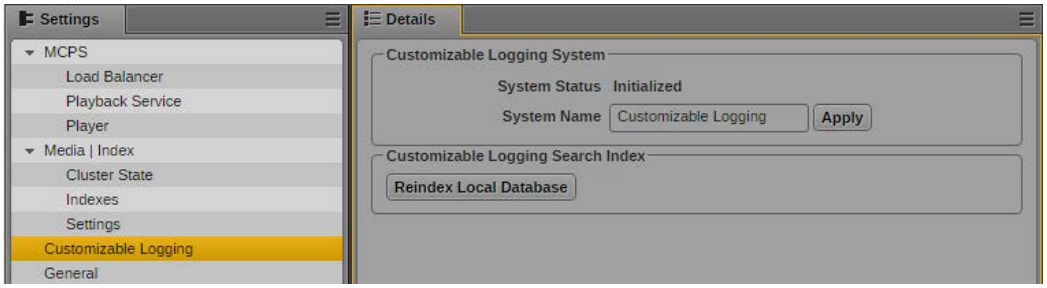
```
/opt/avid/bin/avid_cl_db_recreate
```

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 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 appears 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
```

***Warning**: 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.

PART X: INSTALLING THE 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	15 min
	Process for installing the MAM Connector on an MCS cluster.	
4	Uninstalling the MAM Connector	varies
	In the event that you no longer require Interplay MAM workflows, the MAM Connector software can be easily removed.	
5	Configuring the MAM Connector	5 min
	Once the MAM Connector has been installed, the MediaCentral System Settings must be configured.	

The MAM Connector enables Interplay MAM workflows in MediaCentral UX. The supported configuration for the MAM Connector requires you to install the connector on the MCS server, which is part of your MediaCentral configuration. The MCS server must be fully installed and configured prior to installing the MAM Connector.

The process for upgrading an existing installation and performing a new installation of the MAM Connector are the same. The upgrade process simply overwrites the appropriate files.

Prior to upgrading, note the following:

- Upgrading to MAM Connector v2.7 from a MAM Connecter v2.5 or earlier requires additional instructions. See *the Avid MediaCentral Platform Services ReadMe v2.7.0* for this specialized upgrade process.
- 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. For more information, see **Interplay MAM User** on page 23.
- 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 the ACS Gateway Access Port**” on page 115.
- 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.
- The MAM connector installation process disconnects any user currently logged in to MediaCentral UX. Ensure that all users save their sessions and log off during the installation or upgrade procedures.

Preparing the Software Package

If you have a cluster configuration, complete steps below on the Master and Slave nodes only.

1. Ensure that you have obtained and copied the MAM Connector software to the MCS server(s). If you have not completed these tasks, see **Obtaining the Software** and **Copying Software to the MCS Server** for instructions.

   For the precise installation package name, see the *Avid MediaCentral Platform Services ReadMe*. The MCS software packages are available from the Avid Download Center.

2. Navigate to the directory where the MAM Connector installer has been copied. Example:

   ```
   cd /media/installers
   ```

3. If necessary, unzip the MAM Connector:

   ```
   unzip MediaCentral_MAM_Connector_<version>_Linux.zip
   ```

4. If necessary, unpack the package containing the MAM Connector installations files:

   ```
   tar -xzvf MediaCentral_MAM_Connector_<version>_<build>.tar.gz
   ```

5. Navigate to the newly created directory:

   ```
   cd MediaCentral_MAM_Connector_<version>_<build>_Linux
   ```

Installing the MAM Connector on a Single Server

1. If you have not already done so, navigate to the directory containing the MAM Connector installation script, `install.sh`:

   ```
   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.

3. 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
   ```

4. Restart the avid-interplay-central service:

   ```
   service avid-interplay-central restart
   ```

Installing the MAM Connector in a Cluster

In a cluster deployment, the MAM connector is installed on the Master and Slave nodes. It is not installed on load-balancing nodes.

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 failover. 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

Pacemaker tracks failure counts for various services in a cluster, and a failover from master to slave will automatically take place when a service's threshold is reached. To prevent unintended failovers during installation of the MAM connector, bring the cluster offline first.

1. Begin taking the cluster off-line 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

With all the cluster nodes offline, you are ready to install the MAM Connector software.

Complete the following process on the Master node first. Once complete; repeat the process on the Slave node.

1. If you have not already done so, navigate to the directory containing the MAM Connector installation script, `install.sh`:

   ```
   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.

3. 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
   ```

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.

1. First, bring the master node online:

   ```
   crm node online <node name>
   ```

   Bringing the master node back online starts the Avid Interplay Central service (which was stopped when you put the node into standby).

2. Next, bring the slave node back online:

   ```
   crm node online <node name>
   ```

3. Finally, bring the load-balancing nodes back online:

   ```
   crm node online <node name>
   ```

Checking on 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 AvidIPC resource is online on the master node.
   - Verify the fail-counts for the following resources (at a minimum): AvidIPC, AvidUMS, AvidACS, pgsqlDB.

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, AvidUMS, AvidACS, pgsqlDB (or another)

   <node> (optional) is the node of interest

   ***Note**: 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). For example, for the AvidAll resource, use AvidAllEverywhere. For AvidConnectivityMon, use AvidConnectivityMonEverywhere.*

   ***Note**: You can address the services contained in the postgres resource group (postgres_fs, AvidClusterIP and pgsqlDB) individually, or as a group.*

   For example, to reset the fail-count for AvidALL resource, issue the following command:

   ```
   crm resource cleanup AvidAllEverywhere
   ```

Uninstalling the MAM Connector

In the event that you need to disable MAM functionality, use the following process to uninstall the MAM Connector.

1. If you are in a cluster configuration, see the process above for **Taking the Cluster Offline**.
2. Navigate to the directory containing the MAM Connector "uninstall.sh" script:

   ```
   cd /<path>
   ```

3. 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, repeat uninstallation process on the slave node.

4. Restart the MediaCentral service.

   For a single MCS server:

   ```
   service avid-interplay-central restart
   ```

   For a cluster configuration:

   ```
   crm resource restart AvidIPC
   ```

   Run this command on the Master node first. Once the service has been restarted, repeat on the Slave node

5. If you are in a cluster configuration, see the process above for **Bringing the Cluster Back Online**.

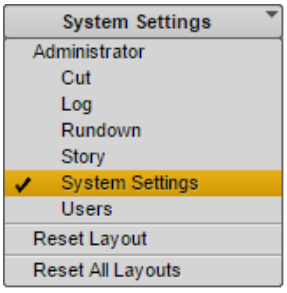
Configuring the MAM Connector

Once the MAM Connector has been installed, additional System Settings must be configured within MediaCentral.

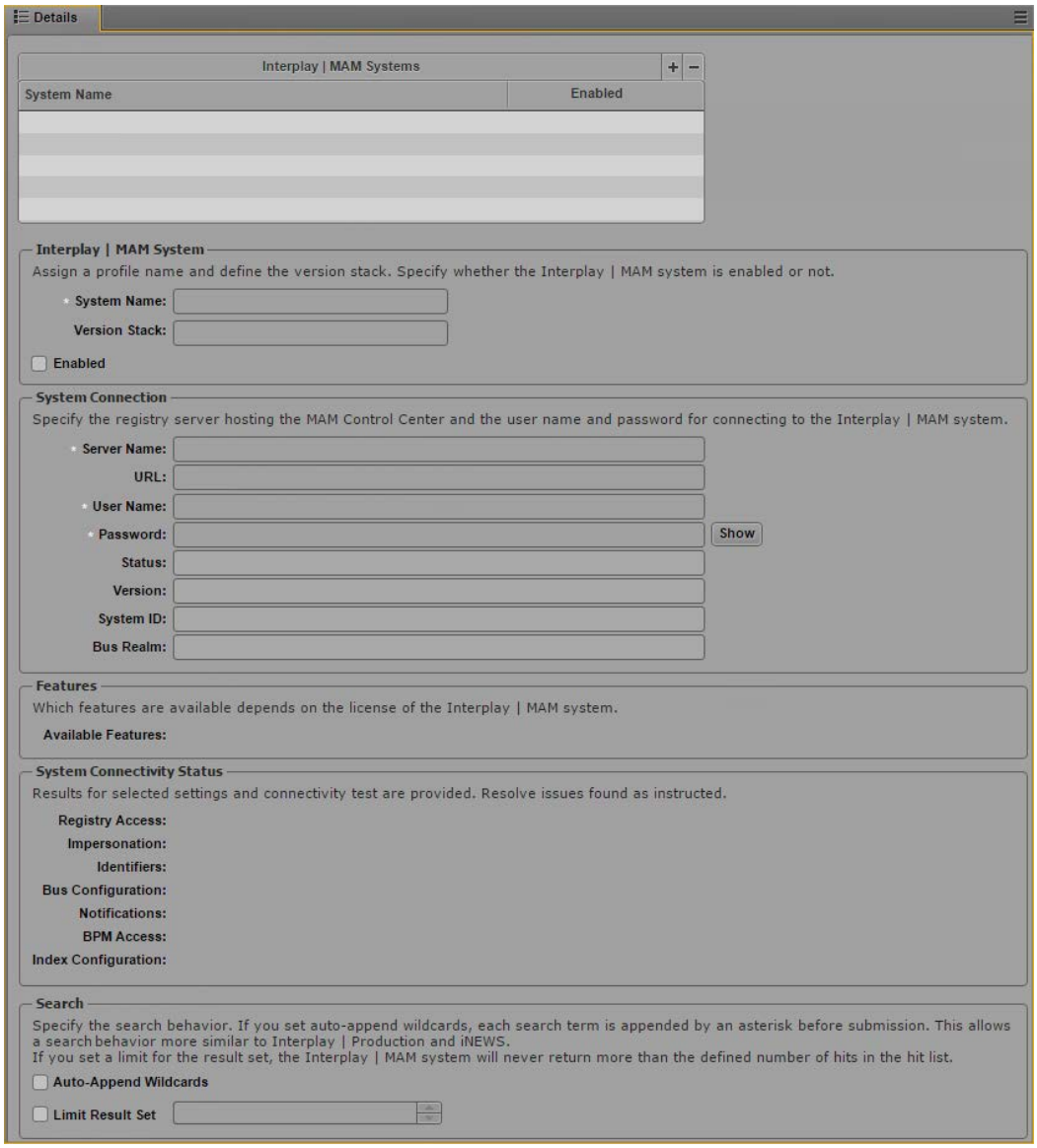
1. Log into MediaCentral.

   For details on this process, see **Logging into MediaCentral UX** on page 94.

2. While logged in as the Administrator, select System Settings from the Layout selector.



3. In the Settings pane, select Interplay | MAM.



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*.

PART XI: MULTI-ZONE CONFIGURATION

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 cover single MCS nodes and MCS clusters that are already established.

The following table describes the topics covered in this chapter:

Step	Task	Time Est.
1	Multi-Zone Overview	1 min
	Provides an introduction to the Multi-Zone concept.	
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.	
8	Dismantling a Multi-Zone Environment	5 min
	Instructions for de-registering the multi-zone environment.	
9	Making Changes to a Multi-Zone Configuration	1 min
	Note regarding making changes to an established Multi-Zone setup.	
10	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”, with the following configuration:

- One MediaCentral server or MediaCentral cluster
- One Interplay Production Engine and/or iNEWS database
- One or more Avid ISIS or Avid NEXIS storage system(s)

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 continue 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 material you found on a remote zone 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:

- **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.

If your organization desires enhanced security, MediaCentral Platform Services can be configured to encrypt data to protect information transmitted data over public networks. If this feature is required, see **Enabling RabbitMQ Data Encryption Across Zones**.

***Warning**: This process 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.*

Verifying the RSA Key Folder

The multi-zone services must be allowed access to remote MCS servers directly and 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 will be located at: `/root/.ssh/`. Assuming 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
   ```

   ***Note**: 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 key to any Load Balancing nodes in any zone.

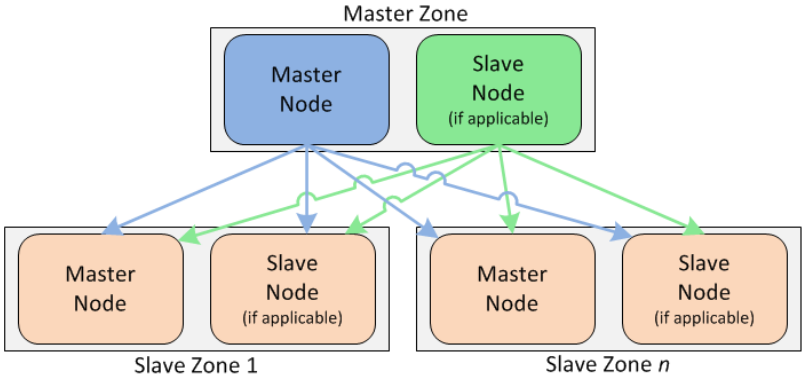
Generate the RSA keys in the Master Zone on the following nodes:

- ☐ 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*.



To Generate and Install 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:

   ```
   ssh-keygen
   ```

   - Press Enter to accept the default file and location
   - 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          |
   |   .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 will respond 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 will respond 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 will respond 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.
   ```

Now multi-zone processes can 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.

   ***Note**: 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.

1. From the Master Node of the Master Zone, make a connection to one of the servers in the Slave Zone:

   `ssh root@<hostname>`

   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:

   `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 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:

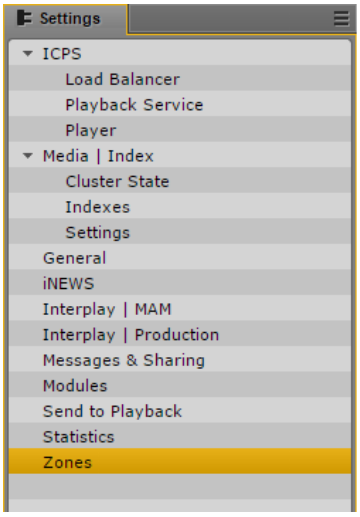
```
exit
```

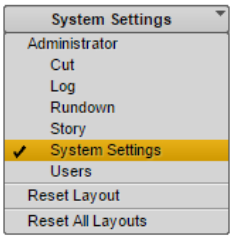
c. If you have additional Slave Zones, repeat these steps for each cluster.

d. Repeat these steps for each Slave Zone cluster from the Slave Node in the Master Zone.

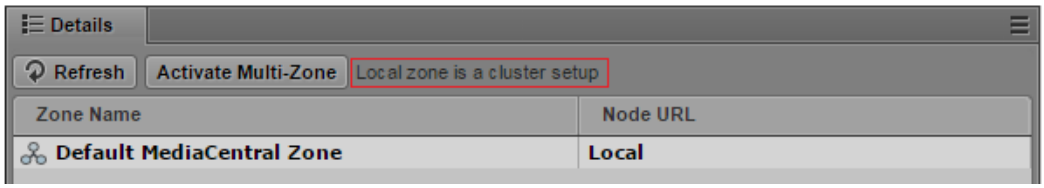
Creating the Master Zone and Initiating Multi-Zone

1. Log in as the Administrator user to the MediaCentral UX instance located in the master zone, and select **System Settings** from the Layout selector.
2. 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.

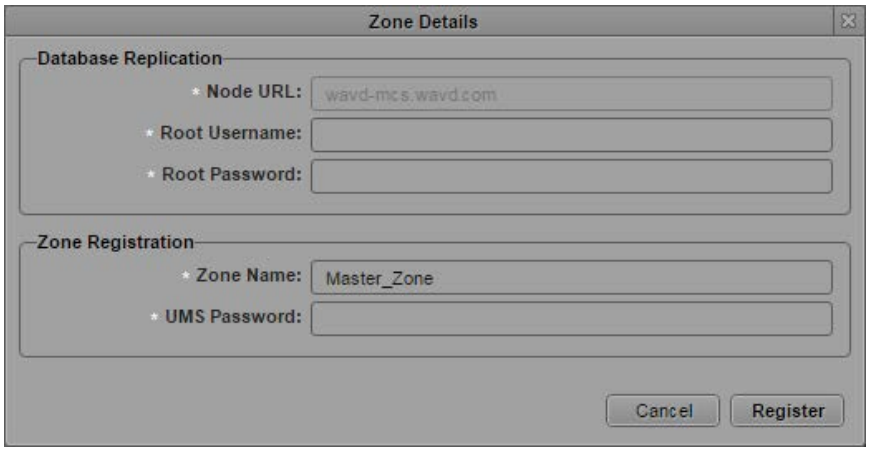


Text to the right of the “Activate Multi-Zone” button indicates if the Master Zone is a single machine or cluster configuration.

3. Click the **Activate Multi-Zone** button.

   A confirmation dialog box appears prompting you to verify that you wish to continue. Click **Proceed**.

   A Zone Details dialog appears.



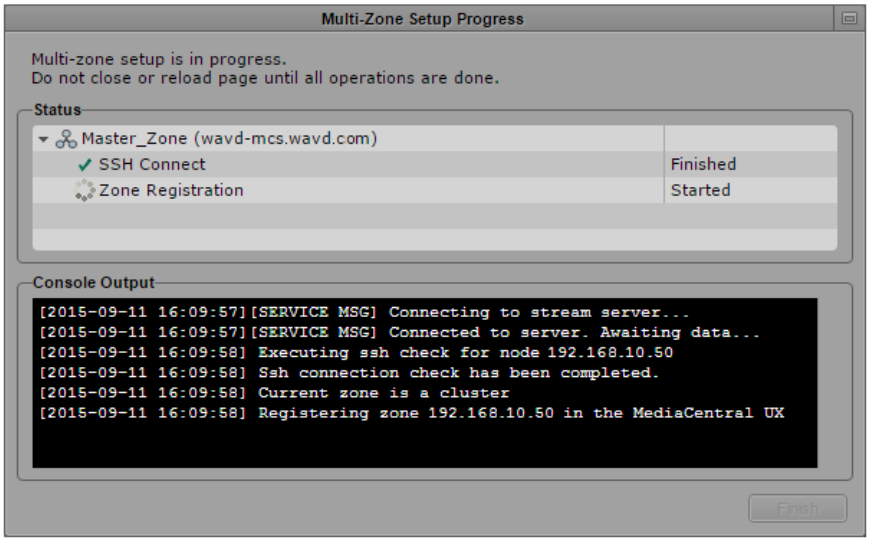
   ***Note**: The Node URL lists the FQDN you entered in the web browser to access MediaCentral UX. This field cannot be altered.*

4. In the Zone Details dialog that appears, enter the following information:

   - Root Username and Root Password: The *root* user credentials for the master zone MCS server.
   - Zone Name: Name of the master zone (e.g. Master_Zone).
   - UMS Password: Enter the MediaCentral UX Administrator password of the master zone.

5. Click **Register**.

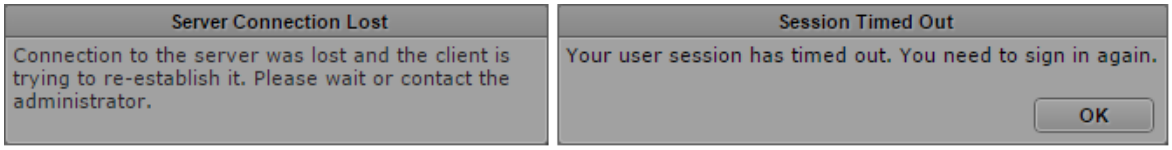
   A dialog appears showing progress of the operations related to zone creation.



   Once complete, a SUCCESS message will appear within the progress window.

6. Click the Finish button to complete the process.

   Some services will be restarted during this period. You may see one or both of the following messages:



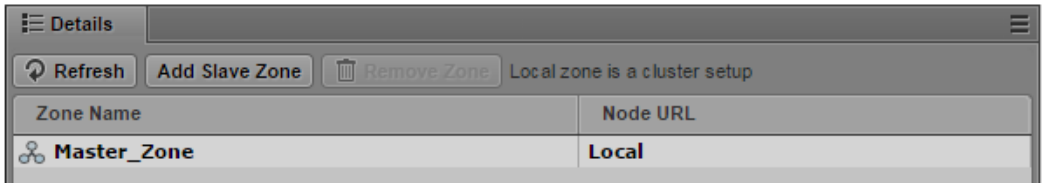
   Click OK in the “Session Timed Out” window.

7. You will be logged out of MediaCentral UX at this time.

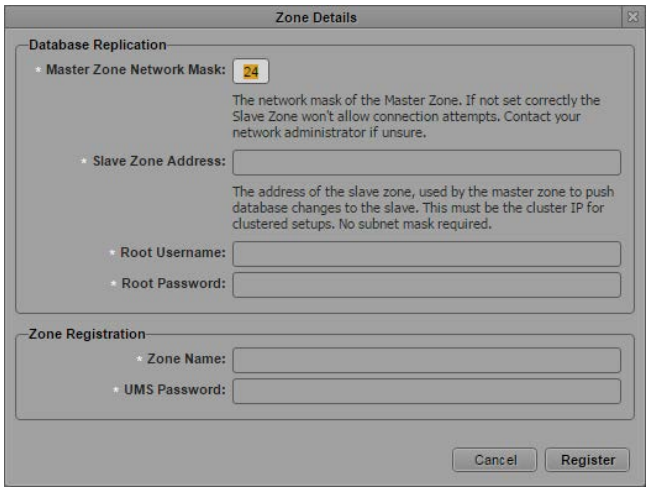
Adding Slave Zone(s) to the Multi-Zone Environment

1. Log 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.

   The Zones Details area now shows the newly created zone (e.g. Master_Zone):



3. Click the **Add Slave Zone** button. The Zone Details dialog appears:



4. In the Zone Details dialog, enter the following information.

   Database Replication:

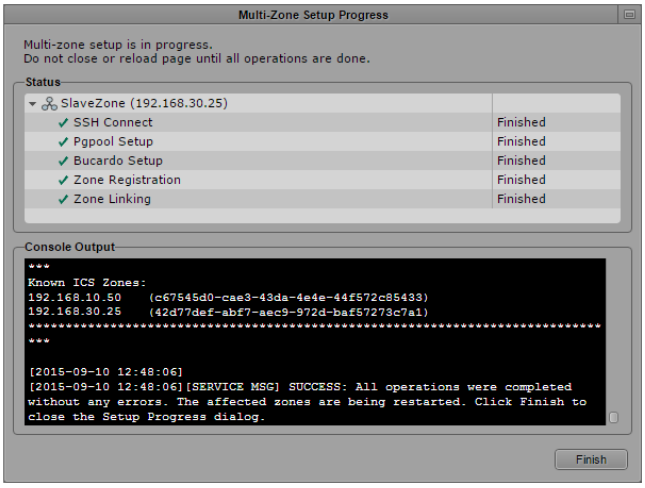
   - Master Zone Network: Specify the IP range for this network (e.g. 23, 24, 25)
   - Slave Zone Address: Specify the IP address of the slave zone. This is either the IP address of a single server or the IP address of a multi-server cluster.
   - Root Username and Root Password: Specify the username (root) 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.

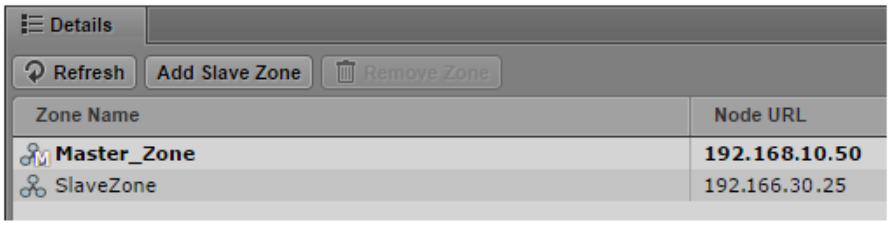


   Once complete, a SUCCESS message will appear within the progress window.

6. Click the Finish button to complete the process.

   ***Note**: Any users logged into the slave zone will be disconnected at this time as services are restarted on the slave zone.*

7. The Zones Details page is refreshed with the new slave zone.



   Note that the master zone is now identified with the letter “M” and the current zone is bolded. The “current zone” is the zone for the machine where you are currently logged in.

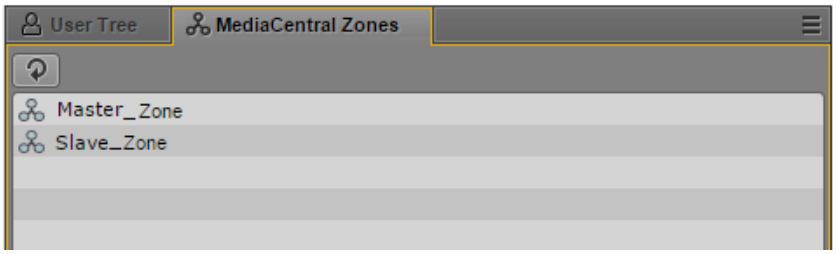
8. Repeat the process to add other slave zones, as desired.

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. Log 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.



4. To validate that a user added to one zone can log 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 **Save** 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, log in to MediaCentral UX in the other zone using the newly created multi-zone user.

   - If you log in to a slave zone, note the user credentials are being validated in the master zone.
   - Notice 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 **PART VI: SHARDED MONGO** on page 133 to reconfigure the zones for a sharded Mongo configuration.

Dismantling a Multi-Zone Environment

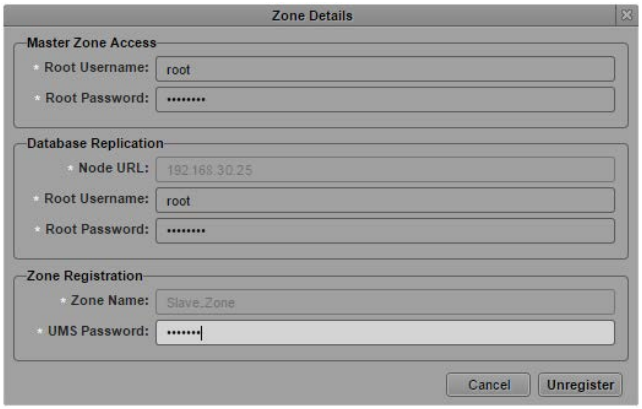
When a multi-zone environment is no longer required, it can be dismantled. Dismantling a multi-zone environment removes all roles for multi-zone users (login credentials remain). If you later use the same user names on independent systems, you need to manually re-assign the roles on each system.

***Note**: 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. Log 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.



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:

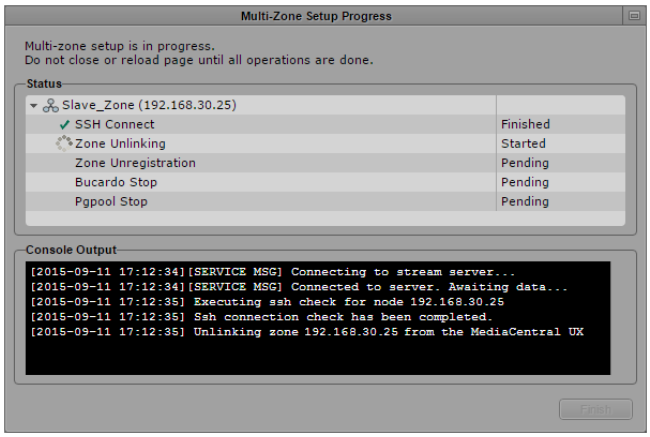
   - Node URL: This field is completed for you. This is the IP address of the MediaCentral instance / cluster in the Slave Zone.
   - Root Username and Root Password: This is the root user of the Slave Zone.

   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.

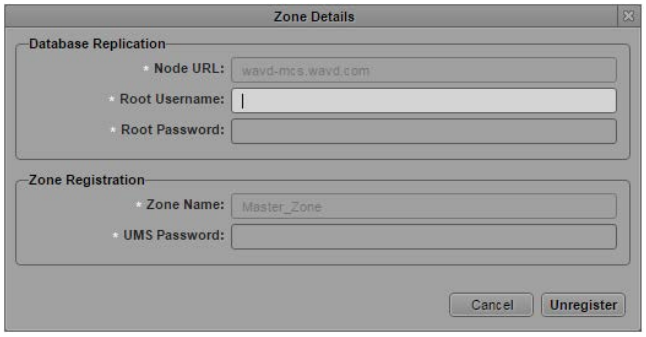
   A dialog appears showing progress of the operations related to slave zone deregistration.



   ***Note**: Any users logged into the slave zone will be disconnected at this time 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.



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:

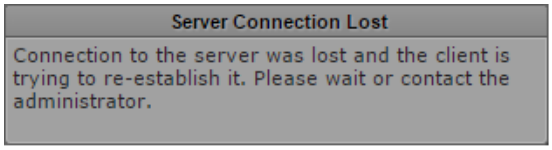
   - Zone Name: This field is completed for you. This is the name of the master zone (e.g. Master_Zone).
   - UMS Password: MediaCentral UX Administrator password for Master Zone.

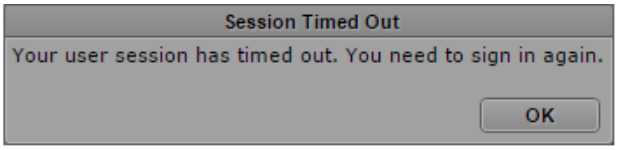
10. Click the Unregister button.

    A dialog appears showing progress of the operations related to master zone deregistration.

    ***Note**: Any users logged into the master zone will be disconnected at this time as services are restarted on the master zone.*

11. Click the Finish button to close the deregistration window.
12. Some services will be restarted during this period. You may see one or both of the following messages:





    Click OK in the "Session Timed Out" window.

13. You will be logged out of MediaCentral UX at this time.

Enabling RabbitMQ Data Encryption Across Zones

During the initial setup of the multi-zone configuration, 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. Altering the configuration file in the following process creates secure multi-zone links in RabbitMQ with a prefix of "amqp**s**://".

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.

***Warning**: This process 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, edit 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.

   ***Note**: Editing the configuration file on cluster load-balancing nodes is not required.*

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, do the following:

Log in to each node of the cluster and type the following command:

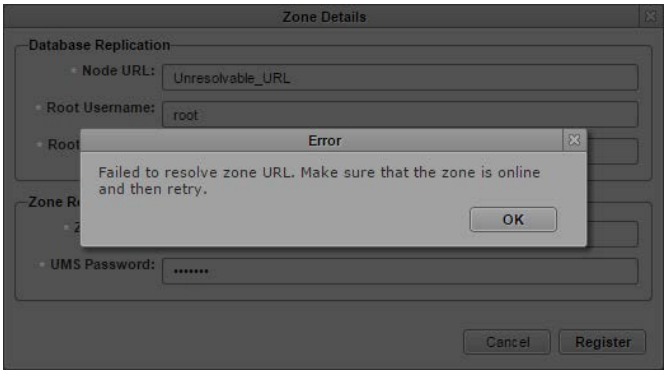
```
service avid-acs-messenger restart
```

Troubleshooting the Multi-Zone Setup

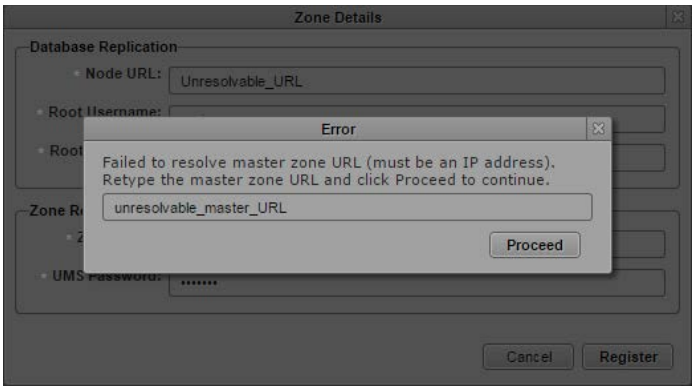
This section contains troubleshooting tips.

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.

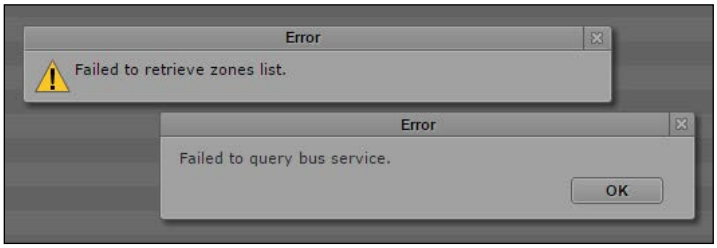


The master zone URL is passed into the zone configuration processes automatically, based on the current URL as shown in the browser. If you receive the following error, it may indicate the browser is using a form that is unreachable to the backend services (e.g. a hostname). Re-enter the address as an IP address and try again.



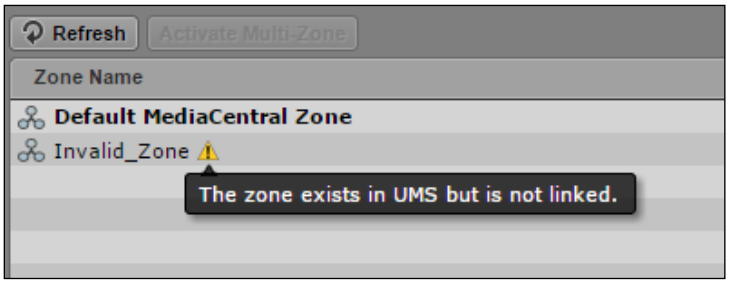
Bus Error

If a "failed to query bus service" error appears, check that the ACS bus is running in a command shell.



Errors in Zone Configuration

An exclamation point next to a zone indicates incorrect configuration.

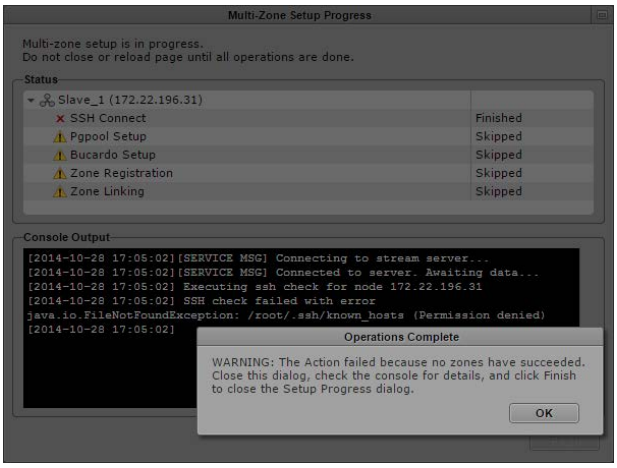


The following table presents typical configuration error messages:

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.
OK

APPENDICES

Appendix A: 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 for Interplay MAM
Working with the Dell RAID Controller
HP DL360p Gen8 Card Placement
Contents of the MCS Installation Package
Enabling Trusted Certificates
Using SNMP Monitoring on the MCPS Server
Port Requirements
Determining the Installed MCS Version
Using the MediaCentral Health Check Script
Enabling the Player Demonstration Web Page
Verifying Cache Directory Permissions
Modifying application.properties
Modifying Configuration Files
Working with Sharded Mongo
Working with the MediaCentral UX Configurator
Backing up and Restoring the MCS Database
Downgrading the Avid Shared Storage Client
Verifying the ISIS Mount
Reconfiguring the ISIS Connection(s)
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

Copying Software to the MCS Server

At various times during the installation, you will need to copy software to the MCS server. The following two processes are provided as examples of how to complete this task:

- ☐ Using a Windows system and a SFTP tool such as WinSCP
- ☐ 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.

Copying Software Using WinSCP

1. Download and install the WinSCP software on a Windows system that has network access to the MCS server.

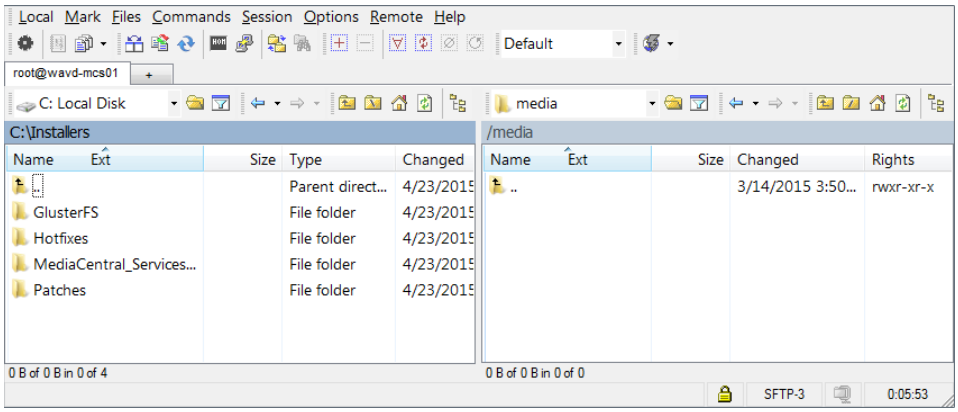
   The WinSCP software can be found at: http://winscp.net.

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.



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_2.7.0`

   ***Note**: 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 and 8.

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 filesystems 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_2.7.0
   ```

   ***Note**: 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_2.7.0`

   For a folder: `cp -R foldername /media/installers/MCS_2.7.0`

10. Once you have finished copying all necessary files, unmount the USB drive.

    ```
    cd
    ```

    ***Note**: In Linux the "cd" command without any arguments takes you directly to the user's home directory. If you are logged in as root, it takes you to the /root directory. RHEL will not unmount the USB drive if it is the current active directory.*

    ```
    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 or the mount command, or both. Then dismount the Linux ISO first, followed by the USB device:

    ```
    umount /sysinstall
    umount /media/usb
    ```

11. Remove the USB drive from the server.

    ***Caution**: 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 for Interplay MAM

MCS supports MediaCentral 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.

For the most part the steps provided in the main body of this guide for installing and configuring MCS on HP and Dell servers are easily generalized to other hardware. The primary difference 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". In the case of Avid MediaCentral Platform Services, the known hardware refers to the HP and Dell platforms.

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.

> ***Note**: 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 will require 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.

> ***Note:** 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).*

Non-HP / Dell Installation Notes

The following notes pertain to the main installation steps for non-HP hardware.

The section contains the high-level steps 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.

1. Configure the server hardware:
    a. Create a RAID 1 (mirror) for the system disk using the hardware BIOS utilities.
    b. If possible, set the date and time in the system BIOS before installing RHEL. Otherwise, set the clock at the appropriate stage in the RHEL installation process.
2. Install RHEL manually:
    a. Select BASIC SERVER during the RHEL installation process.
    b. When prompted to create storage, create two partitions on the OS drive. One partition is for RHEL. The other one is used by DRBD. The DRBD partition should be 20GB in size.

    Note: *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.*
3. Mount the RHEL installer:

    You will need to mount 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)

    Note*: RHEL will automatically create 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. Example:

    ```
    mkdir /media/RHEL
    ```

    Note*: If needed, see Copying Software to the MCS Server for instructions for mounting a USB drive.*

    b. Copy the .iso to the newly created folder.

    ```
    cp /path/rhel-server-6.5-x86_64-dvd.iso /media/RHEL
    ```

    c. Mount the Red Hat Enterprise Linux .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 MCS.
    a. Copy the MediaCentral Platform Services installation package to your server using your desired method.

       For more information, see **Copying Software to the MCS Server**.

    b. If necessary, unzip the installation package:

       ```
       unzip MediaCentral_Services_<version>_<build>_Linux.zip
       ```

    c. Change directories to the MediaCentral_Services foler 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.

Note Regarding Cluster Configurations:

When running the drbd_setup script, the following error has been reported at sites not using the MCS Installation USB Drive to install RHEL and MCS:

```
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 DRBD encountered an issue with the sda2 partition. If this message occurs, ensure that sda2 is at least 20GB in size. If the error persists, the following process can be used to wipe the sda2 partition. Complete this process on the master and slave nodes only:

1. Log in to RHEL as the 'root' user.
2. Ensure that the drbd service is not running by stopping the service:

   ```
   service drbd stop
   ```

3. Navigate to the drbd directory and delete the "r0.res" file:

   ```
   cd /etc/drbd.d
   rm r0.res
   ```

4. Delete the "r0.res" file
5. Enter the following command to zero the sda2 partition:

   ```
   dd if=/dev/zero of=/dev/sda2 bs=512k count=10000
   ```

   ***Note**: This command is destructive, so take care when entering the command.*

6. Once completed on both master and slave nodes, run the drbd_setup script and proceed with the installation as instructed in the main body of this guide.

Working with the Dell RAID Controller

This section provides information on 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

1. 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.

2. From the **Create Virtual Disk** page select **Select Physical Disks**.

3. Put check marks in the appropriate Physical Disk boxes.

   a. For the RAID 1 (system disk) this should be 00:01:00 and 00:01:01
   b. For the RAID 5 (optional cache disk) this should be 00:01:02 through 00:01:07.

4. Select **Apply Changes**.

   A confirmation screen indicates success.

5. From the **Create Virtual Disk Page**, select **Create Virtual Disk**.

   You may need to scroll down the page to see the link.

6. From the Warning page, confirm you selection and select Yes.

   A confirmation screen indicates success.

7. Return to the **Virtual Disk Management** page and select **View Disk Group Properties** to view your changes.

   a. You should see a Virtual Disk 0 (the RAID 1) and a Virtual Disk 1 (the RAID 5).

8. Return to the **Integrated RAID Controller Configuration Utility** page.

9. From the **Integrated RAID Controller Configuration Utility** menu choose **Controller Management**.

10. From the **Controller Management** menu choose **Change Controller Properties**.

11. 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.

12. 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.

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.

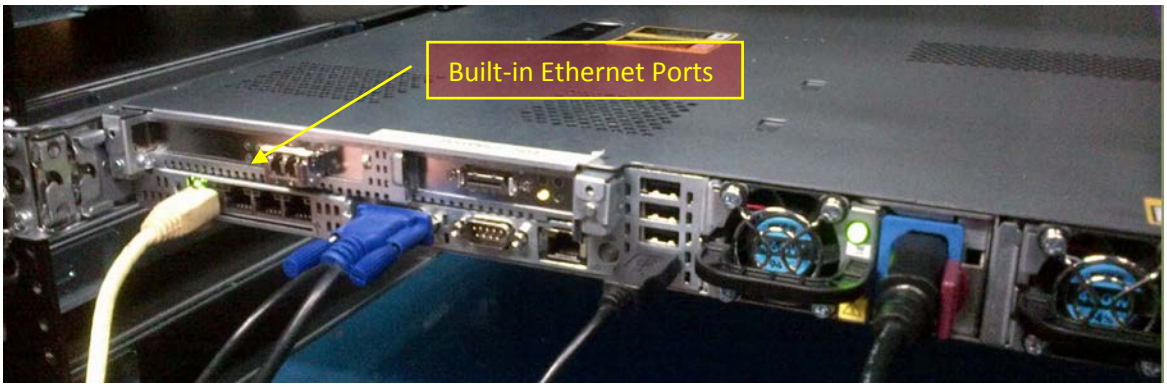
HP DL360p Gen8 Card Placement

Connecting to non-ISIS Proxy Storage

Interplay MAM deployments where browse proxies reside on non-ISIS storage do not require additional NIC cards. They make use of the Ethernet ports built in to the HP server. Visually verify that one of the built-in ports is connected to the network. For a 10GigE connection to non-ISIS storage, use a 10GigE NIC of your choosing.

> ***Note**: If MAM browse proxies reside on an ISIS, the connection to the ISIS must be over a Zone 1, Zone 2, or Zone 3 (recommended) connection, using a GigE or 10GigE network interface.*

HP DL360 Gen8 backplane (showing built-in Ethernet ports):

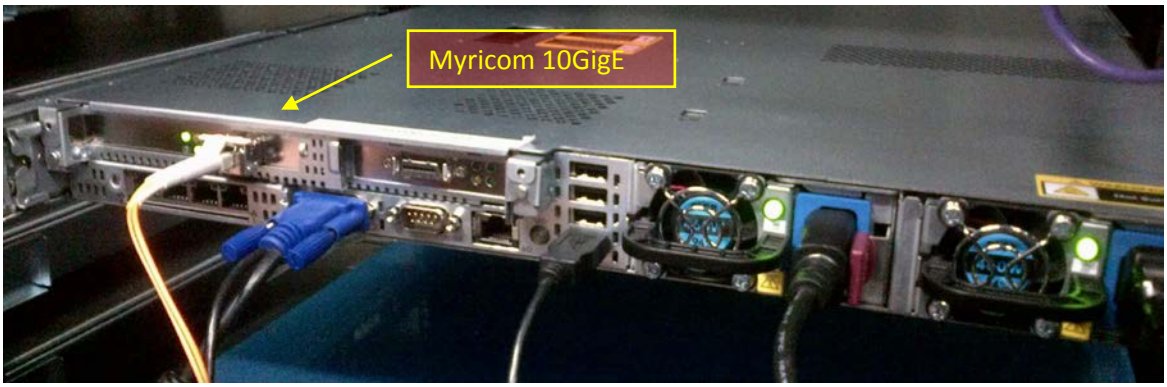


> ***Note**: This applies to Interplay MAM deployments only.*

Connecting to ISIS Proxy Storage

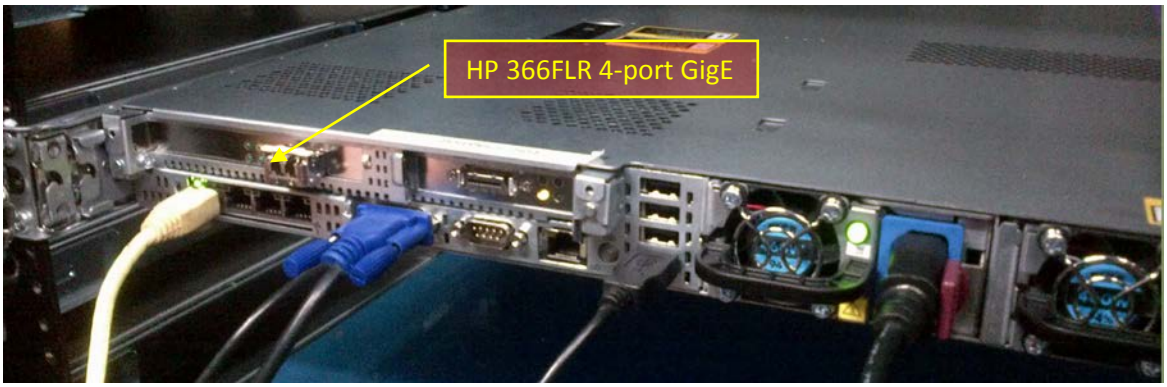
The HP DL360 G8 has a full height PCI slot in the upper left corner. Use this slot for either the Myricom 10GigE or the HP NC365T 4-port GigE NIC. The “built-in” Ethernet ports can also be used, if the server is provisioned with the HP 366FLR 4-port GigE NIC.

HP DL360 Gen8 backplane (indicating Myricom 10GigE):



HP DL360 Gen8 backplane (indicating HP NC365T 4-Port GigE):

HP DL360 Gen8 backplane (indicating HP 366FLR 4-port GigE):



Contents of the MCS Installation Package

The MCS installation package is a ZIP file with a name of the form:

MediaCentral_Services_<*version*>_Linux.zip

For the precise installation package name, see the *Avid MediaCentral Platform Services ReadMe*.

The ZIP file contains 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 It outputs version/build information for the following processes: • 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”) • System ID: An 11-digit number used in support calls that you enter when configuring MediaCentral • ICS Installer - MediaCentral installer The MediaCentral version information is also available in the user interface in the Home -> About box. Once MCS is installed, a symlink is created and you can simply type the following to execute the script: ics_version Starting with MCS v2.6, additional information is also included: • The server’s cluster status • Media Index and multi-zone information • Media | Distribute version information (if installed) • MAM Connector version information (if installed) • Closed Captioning Service version information (if installed)
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.
ks.cfg, ks_upgrade.cfg	The Avid-supplied kickstart files for fresh installations and for upgrade installations.
system-backup.sh	Prepares for an upgrade by backing up important data, including system settings, network settings, the Jetty keystore and application.properties file, and the UMS database.

Enabling Trusted Certificates

For security, MediaCentral uses the Secure Sockets Layer (SSL) for its server-to-browser connections. This is indicated by https:// in the browser address bar, rather than the usual http://. (Some browsers 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

Using SNMP Monitoring on the MCPS Server

The Avid System Monitor application and MCS server can be configured to collect information from the MCS server. This allows you to monitor the status of mandatory MCS services and display graphs for activities such as CPU usage, network usage, and system memory usage. The following items are graphed over time in the Avid System Monitor web page interface:

- Average CPU load
- Number of CPU interrupts per second
- System uptime
- Swap space (disk space reserved for memory when RAM is fully loaded)
- System memory usage
- CPU usage

Contact your Avid representative for information about Avid System Monitor. A qualified Avid support representative can upgrade an Avid System Monitor system to work with MCS.

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

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: 2.7 (Build xx)
Created on <installer creation date>
```

Some notes on the output:

- The System ID is an 11-digit number used in support calls, entered during system configuration.
- 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
  ```

If Media |Distribute, MAM Connector or the Closed Captioning Service 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
```

***Note**: For precise version numbers for this release, see the Avid MediaCentral Platform Services ReadMe.*

Using the MediaCentral Health Check Script

MediaCentral Platform Services v2.7 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)
- 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.

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 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 248.

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*>”.

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.

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/

Enabling the Player Demonstration Web Page

The player demonstration web page (*http://<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).

> ***Note**: 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 http, 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/uninstall 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 248.

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-dev*el RPM:

   ```
   rpm -ivh /opt/avid/Packages/maxcut-devel-<version>-
   <build>.x86_64.rpm
   ```

   Recall that tapping the tab key invokes the Linux autocomplete functionality and ensures accuracy when typing long file names.

   Some feedback appears 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:

   http://<*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.

7. To erase/remove the package (should you wish to uninstall):

   ```
   rpm –e maxcut-devel
   ```

To move the player demonstration web page to a secure location:

```
mv /var/www/html/player/index.html  /root
```

Verifying Cache Directory Permissions

As part of the installation process, a number of cache directories were created. Directory ownership and permissions were set. In this section, you verify the permissions are set correctly.

> ***Note**: This procedure is only necessary for a cluster deployment. Do not use this procedure for a single node deployment. Some directories may not be present, as they are created automatically in a running system. Adjust the steps accordingly.*

To verify cache directory permissions:

1. Verify the ownership and permissions for of all cache directories:

   ```
   ls -la /cache
   ```

   Output similar to the following ought to be presented:

   ```
   drwxrwxrwx   9 maxmin maxmin 4096  Sep 3 14:30 .
   dr-xr-xr-x  33 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	As above.
/cache/render	Automatically created by MCS processes with first multicam playback.

   For a complete description of all cache directories, see the *MediaCentral Platform Services Concepts and Clustering Guide*.

2. The following directories must be owned by user *maxmin*:

   ```
   /cache
   /cache/download
   /cache/fl_cache
   ```

3. The following directories must have the SGID special bit set:

   ```
   /cache/download
   /cache/fl_cache
   ```

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:

1. Log in to the MCS server as the 'root' user. If you have a clustered configuration, log into the master node.
2. Navigate to the following directory:

   ```
   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. 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 information 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 AvidIPC resource must be restarted.

   ***Note**: This step will disconnect any users currently working on the system.*

   a. If running a single server configuration, issue the following command:

      ```
      service avid-interplay-central restart
      ```

   b. If running a clustered configuration, issue the following command on 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
```

See **Validating the FQDN for External Access** for more information.

To Add Passwords for SSL Certificates

For security, MediaCentral 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 2.5 and higher uses a different process for creating the SSL certificates that does not involve altering the application.properties file.

See the article on configuring SSL Certificates on the Avid Knowledge Base for more information.

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;
```

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.

Detecting 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 black gaps in the video. If the system detects black gaps, one of the following occurs, 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 black gaps and retry the STP operation.

***Note**: 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.

Modifying Configuration Files

The MCS server's /usr/maxt/maxedit/etc/ directory contains multiple .cfg files which govern the behavior of the MediaCentral Services player. These files can be modified to include customized modifications.

For example, the edit.cfg file can be altered to specify a network adapter for client connections. In this case, you would add the adapter name to <service_interface></service_interface>:

```
<service_interface>eth2</service_interface>
```

In most cases the configuration files do not require any modification. Only alter the files if instructed to do so by Avid.

Editing a Configuration File

If modifications to the configuration files are necessary, the following process can be used to make the required changes.

To edit a configuration file:

1. Log in to the MCS server as the 'root' user.
2. Open the configuration file for editing:

   ```
   vi /usr/maxt/maxedit/etc/filename.cfg
   ```
3. Make any changes to the file as required by Avid for your environment.
4. Once complete, save and exit the vi session. Press <ESC> and type: `:wq`
5. If you are running a clustered configuration, repeat steps 1 – 4 on all cluster nodes.

   ***Note**: Alternatively, the modified files can be copied to all other nodes.*
6. 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
   ```

Updating the Configuration File

During a system upgrade, the MCS installer checks the configuration files to determine if any modifications have been made. If no modifications are found, the files are overwritten. If the installer finds a modified file, the original "*filename*.cfg" is left unaltered and a "*filename*.cfg.rpmnew" is created in the same directory. The installer script will also inform that user of the file .rpmnew creation:

```
warning: /usr/maxt/maxedit/etc/edit.cfg created as
/usr/maxt/maxedit/etc/edit.cfg.rpmnew
```

To ensure the system is using the most recent version of the configuration file, the modifications made to "*filename*.cfg" must be migrated to "*filename*.cfg.rpmnew".

To update a configuration file:

1. Log in to the MCS server as the 'root' user.
2. List the contents of the /usr/maxt/maxedit/etc/ directory:

   ```
   ls /usr/maxt/maxedit/etc/
   ```

   If any configuration files have been modified prior to the upgrade, both a *filename*.cfg and a *filename*.cfg.rpmnew file will exist in this directory.

   If a *filename*.cfg.rpmnew file is present, continue to step 3.

   If you do not see a .rpmnew file, no custom modifications were made and this process does not need to be completed.
3. You will need to compare the contents of the two files and migrate any custom modifications from *filename*.cfg to *filename*.cfg.rpmnew. To accomplish this task, open a second connection to the MCS server through a SSH client such as PuTTY.
4. In the first SSH window, list the contents of the *filename*.cfg file:

   ```
   cat /usr/maxt/maxedit/etc/filename.cfg
   ```
5. In the second SSH window, open *filename*.cfg.rpmnew for editing:

   ```
   vi /usr/maxt/maxedit/etc/filename.cfg.rpmnew
   ```
6. Compare the contents of the files and migrate any customizations to the .rpmnew file.
7. Once complete, save and exit the vi session. Press <ESC> and type: `:wq`
8. Rename the existing *filename*.cfg to *filename*.cfg.old:

   ```
   mv filename.cfg filename.cfg.old
   ```

   ***Note**: Alternatively, the previous copy of the filename.cfg file could be deleted at this time as it is no longer necessary.*
9. Rename the *filename*.cfg.rpmnew file to *filename*.cfg:

   ```
   mv filename.cfg.rpmnew filename.cfg
   ```
10. If you are running a clustered configuration, repeat steps 1 – 9 on all cluster nodes.

    ***Note**: Alternatively, the modified file or files can be copied to all other 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
    ```

Working with Sharded Mongo

This section includes additional topics that are not covered in the installation process.

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. The following is a list of options and example output of the script:

mongo-checker [command] [options]

command:

check-shard-status	Displays important information about setup

options:

-u=<user>	MongoDB admin user name (example: -u=admin)
-p=<password>	MongoDB admin password (example: -p=AvidAdmin_123!)

Example output of the status command:

```
mongo-checker check-shard-status -u=admin -p=AvidAdmin_123!

------------------------------------------------------------------------
shard0
------------------------------------------------------------------------
Hostname            | state      | health  |   priority |      votes
------------------------------------------------------------------------
 wavd-mcs01:27100   | PRIMARY    |      up |          2 |          1
 wavd-mcs02:27100   | SECONDARY  |      up |          1 |          1
 wavd-nyc:27100     | SECONDARY  |      up |          0 |          1
------------------------------------------------------------------------
shard1
------------------------------------------------------------------------
Hostname            | state      | health  |  priority  |      votes
------------------------------------------------------------------------
 wavd-nyc:27101     | PRIMARY    |      up |          2 |          1
 wavd-mcs01:27101   | SECONDARY  |      up |          0 |          0
 wavd-mcs02:27101   | SECONDARY  |      up |          0 |          0
------------------------------------------------------------------------

CONFIG
------------------------------------------------------------------------
Hostname            | state      |  health |  priority  |      votes
------------------------------------------------------------------------
 wavd-mcs01:28001   | SECONDARY  |      up |          2 |          1
 wavd-mcs02:28001   | PRIMARY    |      up |          2 |          1
 wavd-nyc:28001     | SECONDARY  |      up |          2 |          1
```

This example shows a multi-zone configuration consisting of two zones.

Zone 1 (shard0) consists of a two-node MCS cluster. 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 provides a vote for an election in the event of a failover.

***Note**: As a reminder, mongo clustering and Corosync clustering are independent systems. The sharded Mongo primary node may not always be the corosync master node.*

Zone 2 (shard1) is a single-server configuration (wavd-nyc). 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.

The CONFIG section is independent from the zones. The config service exists on the first seven nodes in the sharded Mongo configuration. In the example above, wavd-mcs02 is the primary config server.

Checking for Stale Nodes

A "stale" node is a member of the sharded configuration whose data has become out of sync with replicated data on the primary node. When a replica member became stale it enters "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 configuration. 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 a different command to check and fix any Mongo stale nodes. The following is a list of options and example output of the script:

mongo-checker [command] [options]

command:

check-stale-nodes	Detect stale replica set members
fix-stale-nodes	Fixes stale replica set members

options:

-u=<user>	MongoDB admin user name (example: -u=admin)
-p=<password>	MongoDB admin password (example: -p=AvidAdmin_123!)
-h	Shows the help options for this command

Example output:

The following is an example of the `check-stale-nodes` command where a stale node has been identified.

```
mongo-checker check-stale-nodes -u=admin -p=AvidAdmin_123!

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.
```

To fix the stale node, run the mongo-checker command from any node with the "fix" option:

```
mongo-checker fix-stale-nodes -u=admin -p=AvidAdmin_123!
```

Using the mongo_setup Script

The mongo_setup 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.

Command options:

- `mongo_setup`

  Running the setup command with no options collects data about the system and displays it on the screen.

  In a multi-zone configuration the script is run in 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_setup -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.

  Where <file> is the user designated name of the csv file. Example usage:

  ```
  mongo_setup -eWAVD.csv
  ```

- `mongo_setup -c`

  The –c switch instructs the script to update the configuration file: `hosts`. This command assumes the user has already run the script without any commands and has verified that the configuration information printed to the screen is accurate.

- `mongo_setup -c<file>.csv`

  Using the –c switch in combination with a file name instructs the script to update the "`hosts`" configuration file using the contents of the specified .csv file.

  Where <file> is the user designated name of the csv file. Example usage:

  ```
  mongo_setup -cWAVD.csv
  ```

- mongo_setup –d

  The –d switch created a debug output that can be used for troubleshooting.

As discussed in **PART VI: SHARDED MONGO**, when used with the -c switch, the mongo_setup 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 `setup.sh` script to configure the system.

Uninstalling the Sharded Mongo Arbiter for Windows

An installer was created to assist in the configuration and creation of the arbiter for Windows systems. However, the software removal process must 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
      ```

      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:

   ***Note**: 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 command 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 command 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

The following process details the steps needed to remove the Mongo arbiter from a Linux system. As a reminder, arbiters are required for two-node cluster configurations that are not part of a multi-zone environment.

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 mogo 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**.

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.

    ***Note**: 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.

Using avid-ics

The `avid-ics` script provides a status for a variety of MCS services and systems, including sharded Mongo. Usage:

`avid-ics status` – Provides a status on a variety of Avid systems.

`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-mcs01 ~]# avid-ics status sharded_mongo
 (pid  2388) is running...
 (pid  2435) is running...
 (pid  2550) is running...
```

The following is an example of the command when run on a clustered configuration:

```
[root@wavd-mcs01 ~]# avid-ics status sharded_mongo
 mongod-iam-config-28001 (pid  70965) is running...
 mongod-iam-shard0-27100 (pid  69023) is running...
 mongos-iam-27018 (pid  72538) is running...
```

This command can be particularly useful for a multi-zone configuration where they may be more `mongod-iam-shard` services.

For more information, see "Using the avid-ics Utility Script" in the *MediaCentral Platform Services Concepts and Clustering Guide*.

Starting Over

If you have identified a problem with the sharded Mongo environment, and have exhausted standard troubleshooting techniques, it is possible to recreate the sharded Mongo configuration from scratch by removing all configuration files from each node.

To remove the sharded mongo configuration, run the `clean_sharded_mongo` command on all Mongo shards (including the master node of the master zone in a multi-zone configuration):

```
/opt/avid/installer/ansible/clean_sharded_mongo -f
```

The –f option indicates you want 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.

In cluster configurations, the script places the AvidIam resource in an unmanaged mode which eliminates errors due to failed (stopped) services.

If you need assistance with this command, run the command with the –h option:

```
/opt/avid/installer/ansible/clean_sharded_mongo -h
```

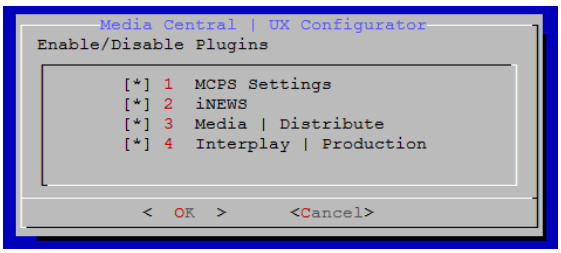
Once these steps are complete, proceed through the sharded Mongo configuration process that is appropriate for your environment. For more information, see **PART VI: SHARDED MONGO**.

Working with the MediaCentral UX Configurator

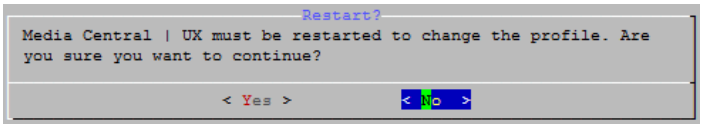
The MediaCentral UX Configurator enables or disables functionality available in MediaCentral UX. The standard features that appear in the tool are:

- MCPS Settings
- iNEWS
- Interplay | Production

Additional features might also appear in the Configurator. However, these features only appear after additional software has been installed on the MCS server.



When enabling or disabling a feature, the following window will appear:



If you select Yes, the avid-interplay-central service will be 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 will disconnect 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. When making a change through the Configurator on a functional cluster, complete the following:

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 failover 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 the MCS System Settings and the MCS 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* utiliy 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
```

> ***Note**: 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 248.

2. Stop pacemaker on both nodes:

   ```
   service pacemaker stop
   ```

3. Start DRBD on both nodes:

   ```
   service drbd start
   ```

4. Make the master node the DRBD *primary* (on the master node):

   ```
   drbdadm primary r0
   ```

5. Mount the DRBD drive on the master node:

   ```
   mount /dev/drbd1 /mnt/drbd
   ```

6. Start the PostgreSQL database on the master node:

   ```
   service postgresql-9.1 start
   ```

7. 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.

8. Stop PostgreSQL on the master node:

   ```
   service postgresql-9.1 stop
   ```

9. Unmount the DRBD drive on the master node:

   ```
   umount /mnt/drbd
   ```

10. Stop DRBD on both nodes:

    ```
    service drbd stop
    ```

11. Restart Pacemaker (which restarts all needed services) on both nodes, master node first, slave node second:

    ```
    service pacemaker start
    ```

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 v2.7 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. Note the current version of the installed shared storage client software:

   ```
   rpm -qa | egrep -i 'isis|nexis'
   ```

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. Note the current version of the installed shared storage client software:

   ```
   rpm -qa | egrep -i 'isis|nexis'
   ```

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. Replace the existing shared storage client with the previous version:

   ```
   rpm -e AvidNEXISClient
   ```

   ```
   rpm -Uvh /opt/avid/Packages/AvidISISClient-
   <version>.el6.x86_64.rpm
   ```

   Repeat this command 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'
   ```

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.

Verifying the ISIS Mount

The validity of the ISIS mount is initially authenticated during the configuration procedure. In that procedure, the Status of the ISIS connection changes from “Disconnected” to “Connected”.

However, it is possible to verify the ISIS 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 ISIS mount(s):

1. Verify the status of the avid-isis service:

   ```
   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 filesystems of type *fuse.avidfos* (the ISIS filesystem):

   ```
   mount -t fuse.avidfos
   ```

   The system responds with output showing the ISIS mounts, 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 an ISIS called *wavd-isis* mounted at /isis/wavd-isis. "Fuse" is the RHEL filesystem type reserved for third-party filesystems.

3. The Linux *df* command displays disk usage information for all the mounted filesystems:

   ```
   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 ISIS and its workspaces by navigating it as you would any Linux filesystem.

   For example, for the sample output shown above, to view the workspaces available to the MCPS player, list the contents of the mounted ISIS:

   ```
   ls /mnt/ICS_Avid_Isis/wavd-isis
   ```

Reconfiguring the ISIS Connection(s)

When you set up MCS for the first time you configure a network interface to be used for playback of video assets. For a MediaCentral UX and/or Media Composer UX deployment, for example, you configure a GigE or 10GigE connection to the ISIS. If at a later date you decide to change the network interface, this section provides the instructions.

To reconfigure the ISIS Connection(s):

1. Install the new card.

   See **Network Interface Cards and Network Connections** on page 15.

2. Verify the NIC interface names using the RHEL Network Configuration tool.

   See **Identifying NIC Interfaces and Connecting the Network Cable** on page 68.

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.

   See **(HP Only) Swapping NIC Interface Names** on page 69.

4. If running an HP server, remove the MAC address hardware references for the swapped ports from the corresponding *ifcfg-ethX* files and reboot.

   See **(HP Only) Removing the MAC Address Hardware References** on page 71.

5. Log in to MediaCentral UX with administrator privileges and update the ISIS 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".

   See **Playback Service Settings** on page 102.

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 routers do not support multicast (i.e. are not multicast 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.

> ***Note**: If you are converting an existing multicast cluster to unicast communication, skip Step 1 of the following process.*

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.

Configuring Unicast Cluster Communication

This process assumes that the following steps from the **PART V: CLUSTERING** section of this guide have already been completed:

- **Cluster Overview**
- **Configuring the Player System Setting**
- **Configuring DRBD**

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 not required in this command.
   - *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 in this command

   ***Note**: 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. Once the cluster services have been stopped on the slave node, stop the services on the master node:

   ***Note**: Prior to running this command, you can confirm the status of the slave and load-balancing nodes through the Cluster Resource Monitor, crm_mon. All non-master nodes should report as “OFFLINE”.*

   ```
   service pacemaker stop && service corosync stop
   ```

5. Using the example above 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.

6. 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.

7. 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>"
   ```

   See “Starting the Cluster Services on the Master Node” for details (and the appropriate form of the *setup-cluster* command).

8. 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
   ```

9. 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
   ```

Reconfiguring MediaCentral Settings in a Cluster

If you reconfigure any MediaCentral System Settings (e.g. adding/removing an ISIS 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 let your users know that playback may 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 log in to MediaCentral 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 failover. 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 crm_mon by pressing CTRL-C on the keyboard.

Appendix B: Configuring Port Bonding for Interplay MAM

Port bonding (also known as link aggregation) combines multiple physical interfaces into a single logical interface. In MediaCentral deployments for MAM, 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. Press **Enter**.
3. Choose the Device Configuration option. 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.

  ***Note**: Mode 4 requires a switch that supports IEEE 802.3ad Dynamic link aggregation. All interfaces must match speed and duplex settings.*

  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"`

- `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`

Appendix C: Configuring iNEWS for Integration with MediaCentral

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

***Note**: Additional files must be edited to ensure proper licensing for iNEWS integration with the MediaCentral mobile application. For more information, see* Appendix D: Avid MediaCentral | UX Mobile Application *on page 255.*

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.

***Note**: 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*".

***Note**: 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.

   ***Note**: 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's server prompt will 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's server prompt will 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** above.

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 MediaCentral middleware 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 middleware (Web application) servers, you will need to add the IP address for each one on individual lines in the story.

   ***Note**: You do not need to add to SYSTEM.CLIENT.WINDOWS the IP addresses of any MediaCentral client computers or devices.*

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's server prompt will 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's server prompt will change back to a dollar sign ($).

Appendix D: Avid MediaCentral | UX Mobile Application

The Avid MediaCentral UX mobile app is a native user interface designed to run on the Apple iPad, iPhone and various Android-based devices. It enables direct, secure access to your station's iNEWS and /or Interplay Production systems.

When connecting to an iNEWS system, users can view and approve news stories, navigate the news directory, play video sequences associated with stories and view a show's scripts in presenter mode (iPad only). Users connecting to Interplay Production systems can browse and play production assets.

The MediaCentral UX mobile app can connect to your environment in one of two ways:

- Wi-Fi
- Carrier-specific cellular service— for example, 3G, 4G or Edge

***Note**: 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 will be accessed from the MediaCentral UX mobile app (iPad, iPhone or Android device). Mobile devices that cannot resolve the FQDN of the MediaCentral server(s) experience issues connecting to the player service. Mobile users are often able to sign into MediaCentral UX, but media playback is not possible or is 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 Gluster has been installed. This is a requirement for streaming to mobile devices.

  See: **Replicating the File Caches using GlusterFS** on page 131.

- ☐ Verify that the Hostname in the MediaCentral "**MCPS> Player**" System Settings has been configured with the system's Fully Qualified Domain Name (FQDN).

  See **Player Settings** on page 104.

- ☐ Confirm that the mobile device can access the MediaCentral server through a Fully Qualified Domain Name (FQDN).

  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.

  See: **Appendix C: Configuring iNEWS for Integration with MediaCentral** on page 252.

- ☐ Verify that Wi-Fi and/or or 3G/4G streams have been enabled on your MCS system.

  See: **Enabling / Disabling 3G and Edge Streams** on page 87.

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*".

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.

   ***Note**: To obtain the correct version of the iNEWS Client module, see the Avid MediaCentral Platform Services ReadMe.*

4. If the version is correct, then close the story. You do not need to complete the rest of the steps in this procedure.
5. If the version is not correct or does not appear, on a new line, add the version of the iNEWS client module that will run on the MediaCentral server.
6. Save the story.
7. 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's server prompt will change to a pound sign (#).

   c. Take the system offline by typing: `NRCS-A# offline`
   d. Reconfigure the system by typing: `NRCS-A# configure`
   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's server prompt will change 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 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.

> ***Note**: 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 /site/config for the Avid Central mobile application:

1. Select all servers.

   > ***Caution**: 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 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
   ```

   > ***Note**: 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.

   ***Caution**: 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. 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’s server prompt changes to a pound sign (#).

   c. Take the system offline by typing: NRCS-A# offline
   d. Reconfigure the system by typing: NRCS-A# configure
   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’s server prompt changes back to a dollar sign ($).

Installing Avid Central on an iOS Device

The following procedure assumes licensing, setup, and configuration of the MediaCentral and iNEWS and / or Interplay Production servers have already been completed.

To install Avid Central on an iPad or iPhone:

1. Open iTunes (the Apple market).
2. Locate the Avid MediaCentral UX mobile application.
3. 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 app on the Apple iTunes Store 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 Avid Central on an Android Device

The following procedure assumes licensing, setup, and configuration of the MediaCentral and iNEWS and / or Interplay Production servers have already been completed.

To install Avid Central on an Android device:

1. Open the Google Play Store
2. Search for "Avid MediaCentral".
3. Select the application and click 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 will need to 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 may want to create a backup of the current version of the app. This will enable 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 will be 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

Appendix E: Avid MediaCentral | UX Desktop

This appendix covers the Avid MediaCentral UX Desktop application. The following topics are included in this guide:

- System Requirements
- Software Installation
- Differences between MediaCentral UX Desktop and the MediaCentral UX web browser experience
- Troubleshooting

Understanding the Desktop Application

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 higher
  - Desktop v1.2 and higher: Adobe Flash Player v18 (**PPAPI**) or higher
- 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 if necessary.

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.

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

   ***Note**: 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.

   ***Note**: 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 a 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

1. Log 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**.

Installing the Client Software for Mac

1. Log 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**.

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 pull-down 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.

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.

   ***Note**: 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.

1. Log 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_1.0.0_Win.exe /s /v"/qb
SERVERLIST="""MCSERVER=http://news-mcs""""
```

Value	Example	Value Description
MCSERVER	"*WAVD Central*"	This is a "friendly" name of the MCS system. This name will appear in the System pull-down 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	http://<*host*>	Where <*news-mcs*> is 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 will report the reason for the failure which could be missed if running the script directly from a folder.

The script will perform 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.

***Note**: 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 Command Line:

1. 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. 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.

4. Press Enter in the command window to begin the installation.

   The silent installer for the application will appear and automatically close when done.

A successful installation should return the following text in the command window:

```
ScriptDIR= C:\Avid_Installers\
Returncode was 0
Install complete.
```

***Note**: If errors occurred during the installation, the Returncode will specify the source of the issue.*

5. Once the installation is complete, close the command window.

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 will appear, followed by the silent installer for the application. Once the installation is complete, the command window will close.

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. See **Editing the Configuration File** for details on creating the config.txt file.
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:
   `<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 will appear:

   ```
   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 installs the supporting infrastructure needed for Active X controls and 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.

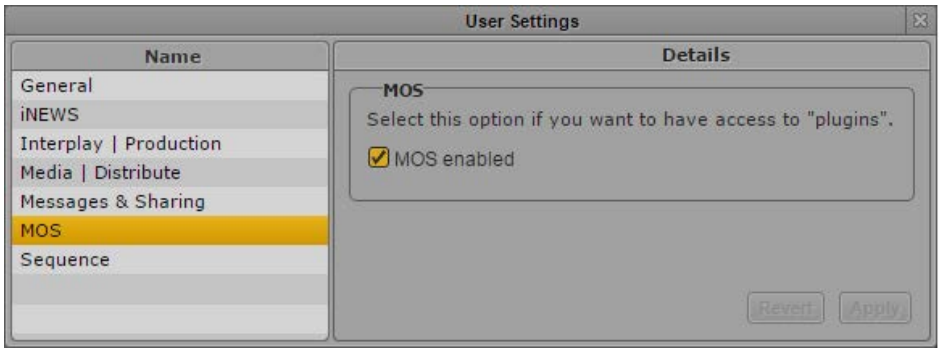
After installation and configuration, plug-ins are listed at the bottom of the Panes menu.

> ***Note**: 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

To use MOS plug-ins, users need to enable a setting in MediaCentral UX:

1. Sign into MediaCentral UX as the user that requires access to MOS plug-ins.
2. Select Home > User Settings > MOS



3. Select the checkbox for "MOS enabled."
4. Click Apply.

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:

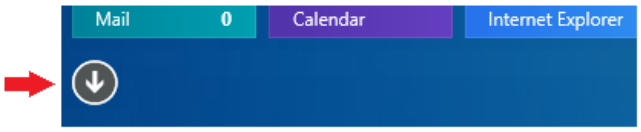
- Launching the Application
- Working with the Menu System
- Accessing Additional MCS Systems
- Selecting a Deep Link

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.

  ***Note**: If you do not see the tile, click the arrow in the bottom-left corner of the Start screen to reveal all installed applications.*



- Mac: The application is located at: Mac HD/Applications/Avid/MediaCentralUX

  ***Note**: For ease of access, you may 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 will ask 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 – This is a user settings that can enabled or disabled to allow usage of MOS plug-ins installed on the user's workstation (personal computer) within MediaCentral UX Desktop.

Systems

- Lists other MCS systems within the organization. See **Accessing Additional MCS Systems** for more detail on this feature.

Help

- About – Provides the version of MediaCentral UX Desktop. Click anywhere outside of the About window to continue working.

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.
- Quit – Closes (quits) the application

View

- Reload – Equivalent to a refresh of a web browser. If you have unsaved work, the system will ask 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

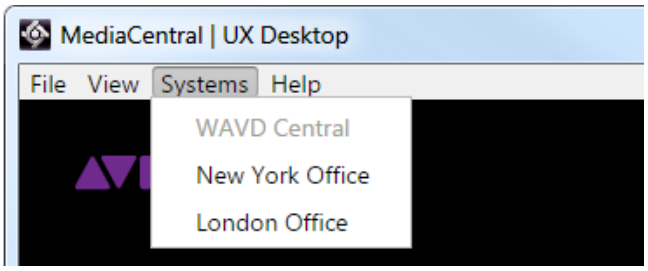
- Lists other MCS systems within the organization. See **Accessing Additional MCS Systems** for more detail on this feature.

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.

***Note**: 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 will open an additional MediaCentral UX Desktop window.

***Note**: 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. Log 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. Log 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 checkboxes (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.

***Note**: 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 in the following location: C:\Users*user*\AppData\Roaming\MediaCentralUX

Appendix F: Enabling MOS Active-X Plug-Ins

This section includes legacy information for enabling MOS Active-X Plug-Ins in:

- ☐ Chrome (v44 or earlier)
- ☐ Internet Explorer (legacy)

***Note**: Chrome v45 depreciated support for the code that enables MOS plug-ins. For workflows that need to continue using MOS plug-ins, see **Appendix E: Avid MediaCentral | UX Desktop**.*

***Note**: As of MediaCentral v2.3, Internet Explorer is no longer a supported browser. This applies to all versions of Internet Explorer.*

***Note**: Active X plug-ins are not supported in the Safari browser.*

Enabling MediaCentral MOS Plug-Ins in 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.

> ***Note**: 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.

  ***Note**: See the Avid MediaCentral Platform Services v2.3 ReadMe for additional information regarding support of Active-X plugins in Chrome.*

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."

> ***Note**: If you are running MCS v2.5 on Chrome v45 or later, this feature will not be available.*

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 Help.

Enabling MediaCentral MOS Plug-Ins in Internet Explorer

The instructions in this appendix were produced for Internet Explorer 9.0.8112.16421 using Google Chrome Frame 65.169.107 on Windows 7 x86_64 SP1. Updates to any of these applications may change the steps below, including the order in which you perform them.

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 will create 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.

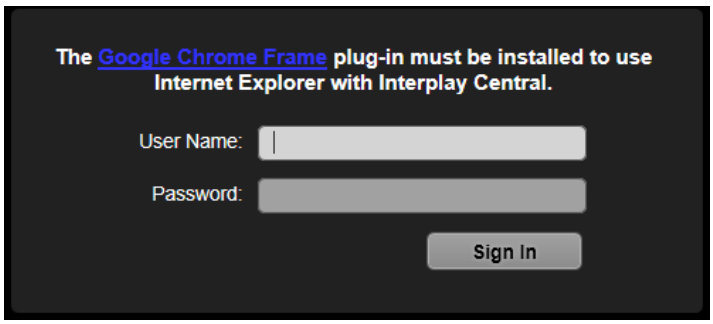
To enable MediaCentral MOS plug-ins in IE:

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 sign-in page informs you that the Google Chrome Frame is required.



2. Install Google Chrome Frame using the link on the sign in page.

   ***Note**: 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 log in as a user for whom MOS plug-ins are enabled.

   ***Note**: To enable MOS for the logged in user, in MediaCentral, 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 say 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 and log in as the same user. Do not download setup.exe again. Sign out of MediaCentral 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.
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 IE, navigate to the MCS server or cluster (e.g. https://<*FQDN*>), and log in as the user for whom MOS plug-ins are enabled.

    Installed ActiveX plug-ins are now visible in MediaCentral, on the Panes menu.

Sample ActiveX Object in the Preferences File

For reference, the full ActiveX object after completion of the procedure is included below. Some values may be different for your particular 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":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCa6DtGBLy26p0nWU7mfBTutgDZpGZw0t
a30LRo1Av6J1LUgL3AxJu5BP4TJxlXXbIKd0H2X6oLgKU3GIw5+r1YKK8BKVfgjpSanEWzg
vWsbjXcnH4XVF8thXYvutkTj5telkhFmOba1UG0zauqMqpnWus9ADGyMGBUIPsTlLhXDwID
AQAB",
               "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
         },
```

Copyright and Disclaimer

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:

Copyright © 1988–1997 Sam Leffler
Copyright © 1991–1997 Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software [i.e., the TIFF library] and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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:

Copyright (c) 1989 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (C) 1989, 1991 by Jef Poskanzer.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

Copyright 1995, Trinity College Computing Center. Written by David Chappell.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. This software is provided "as is" without express or implied warranty.

Copyright 1996 Daniel Dardailler.

Permission to use, copy, modify, distribute, and sell this software for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Daniel Dardailler not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Daniel Dardailler makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Modifications Copyright 1999 Matt Koss, under the same license as above.

Copyright (c) 1991 by AT&T.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

Avid MediaCentral Platform Services 2.7 Installation and Configuration Guide • 10 January 2017 • This document is distributed by Avid in online (electronic) form only, and is not available for purchase in printed form.