HP OpenView Configuration Management

Distributed Configuration Server

for the AIX; Enterprise Linux ES, AS; HP-UX; Solaris; SuSE Linux Enterprise Server; and Windows operating systems

Software Version: 5.00

Installation and Configuration Guide

Document Release Date: April 2007

Software Release Date: April 2007

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

Microsoft®, Windows®, and Windows® XP are U.S. registered trademarks of Microsoft Corporation.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER
Copyright © 1996-1999 Intel Corporation.

TFTP SERVER
Copyright © 1983, 1993
The Regents of the University of California.

OpenLDAP
Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.
Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License
Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License
Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

DHTML Calendar

Documentation Updates

This guide's title page contains the following identifying information:

- Version number, which indicates the software version.
- Print date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition, visit:

ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

The following table indicates the changes that were made to this document since the previously released edition.

Table 1 Changes in This Document

Chapter	Version	Changes
All	5.00	Revised all directory paths. The default directory paths for CM products have been revised to: • `Program Files\Hewlett-Packard\CM` (Windows) And... • `HP/CM` (UNIX)
All	5.00	Removed all references to user interfaces; there is no graphical "configurator" in this version of CM-DCS.
Chapter 2	5.00	Removed the section, CM Distributed Configuration Server Processing, because the CM-DCS configuration and synchronization processes are non-interactive in this version of CM-DCS.
Chapter 3	5.00	Updated this chapter to include the new installation steps that were introduced in this version of CM-DCS.
Chapter 4	5.00	Removed most of the information from Chapter 5, Setting up a Distributed Configuration Server Synchronization, because it pertained to GUI-configuration procedures. The information that is still relevant was combined with Chapter 4, Distributed Configuration Server Security. The result is a revised Chapter 4, The EDMPROF File and CM DCS Security.
Chapter 5	5.00	Removed most of the information from Chapter 6, Configuring Distributed Configuration Server Options, because it pertained

Chapter	Version	Changes
		to GUI-configuration procedures. The information that is still relevant was combined with Chapter 7, Distributed Configuration Server's DMABATCH. The result is a revised Chapter 5, CM Distributed Configuration Server Options and DMABATCH.
Appendix A	5.00	Removed information that is not relevant to this release. This includes version 4.6 messages and logs, and EDMAMS information.

Support

You can visit the HP Software support web site at:

www.hp.com/managementsoftware/services

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction 11

Documentation Map 12

Terminology 12

2 Introduction to the CM Distributed Configuration Server 15

Overview 16

CM Distributed Configuration Server 16

CM Distributed Configuration Server Components 17

Source vs. Destination 17

Two CM Configuration Servers: A Synchronization Pair 19

CM Configuration Server Eligibility 19

Improving Performance using MANAGER_TYPE 20

Domain Ownership 20

Domain Naming Considerations 21

One Owner vs. Multiple Owners 21

One Owning CM Configuration Server 21

Multiple Owning CM Configuration Servers 22

Domain Eligibility 23

Selecting Domains 23

Domain Eligibility Rules 23

CM Distributed Configuration Server Configuration 24

CM Distributed Configuration Server: Batch Mode 24

Synchronization Logs 24

Simultaneous Synchronizations 24

CM Distributed Configuration Server Planning 25

When to Use CM Distributed Configuration Server 25

3 Installing the CM Distributed Configuration Server 27

Two-Phase Installation 28

System Requirements.....28
Platform Support.....28
CM Distributed Configuration Server Directories.....29
Source.....29
Destination.....29
CM Distributed Configuration Server Space Requirements.....30
Installing the CM Distributed Configuration Server.....30
UNIX Pre-Installation Notes.....30
Installing the CM Distributed Configuration Server Source Component.....32
Installing the CM Distributed Configuration Server Destination Component.....33
Post-installation Notes.....39
Setting a Temporary Directory.....39
Source Component.....39
Destination Component.....39

4 The EDMPROF File and CM DCS Security.....41

The EDMPROF File.....42
MGR_STARTUP Section.....42
MGR_DMA Section.....43
Setting up Security.....44
Native Operating-System Security.....44
CM Configuration Server Security Settings.....44

5 CM Distributed Configuration Server Options and DMABATCH..47

CM Distributed Configuration Server Configuration File.....48
Terminology.....48
Configuration Object Equivalents.....50
DMASTATS.....52
ZUSERID.....53
DMABATCH Command-line Options.....54
Reset.....54
Deferred Commit.....55
DMABATCH Scripting Commands.....55
DMABATCH Line Commands.....56
CSID Value Considerations.....57

Results of DMABATCH 57

A Troubleshooting the CM Distributed Configuration Server 59

Logs to Obtain 60

Log Error Messages 60

Log and Object Locations 60

Activating Tracing for CM-DCS 61

CM Distributed Configuration Server Objects and Files 61

CM Distributed Configuration Server Objects 61

CM Distributed Configuration Server Files 62

The EDMAMS Utilities 62

UPDATE_MGRIDS 63

Domain Eligibility 63

B Product Name Changes 65

Index 67

1 Introduction

At the end of this chapter, you will have had the opportunity to:

- Preview which chapters contain which information about the various aspects of the HP OpenView Configuration Management Distributed Configuration Server (CM Distributed Configuration Server).
- Become familiar with some of the terminology that is specific to CM Distributed Configuration Server (CM-DCS).

Documentation Map

The following table provides an overview of this book; this will aid in locating specific information about the CM Distributed Configuration Server.

Table 2 Document Map

Chapter	**Contents**
Chapter 2 Introduction to the CM Distributed Configuration Server	CM Distributed Configuration Server, including: how CM-DCS works; the roles of the two CM-DCS components; CM Configuration Server eligibility, domain ownership, and domain eligibility.
Chapter 3 Installing the CM Distributed Configuration Server	Installing the two CM-DCS components, including system recommendations.
Chapter 4 The EDMPROF File and CM DCS Security	The edmprof file sections that are relevant to CM-DCS; and setting up security for CM-DCS.
Chapter 5 CM Distributed Configuration Server Options and DMABATCH	A look at the CM-DCS configuration file and its options; and the DMABATCH command-line options.
Appendix A Troubleshooting the CM Distributed Configuration Server	Troubleshooting CM-DCS, including logs, tracing, and domain eligibility.

Terminology

Table 3 describes the CM Distributed Configuration Server-specific terms that are used in this document. Review these terms and their descriptions in order to better understand the concepts and materials contained herein.

Table 3 **CM Distributed Configuration Server Terminology**

Term	**Description**
CM Distributed Configuration Server	The CM Distributed Configuration Server is an extension of the CM Configuration Server. It synchronizes CM Configuration Server Databases that are running on separate (CM-DCS-enabled) machines across an enterprise.
CM Integration Server	The HTTP file server of Configuration Management. It gets installed on a Source CM Configuration Server in order to facilitate multiple concurrent file transfer sessions and the creation of the container file.
Source CM Configuration Server (**master**)	In a CM-DCS synchronization, the CM Configuration Server from which the Destination CM Configuration Server will receive database changes.
Destination CM Configuration Server (**slave**)	In a CM-DCS synchronization, the (target) CM Configuration Server on which CM Configuration Server Database changes will be replicated. **Note**: This is *always* a replica of the Source database.
Synchronization	The replicating of administrator-specified domains from one CM Configuration Server Database (Source CM Configuration Server) to another (Destination CM Configuration Server).
Peer Synchronization	Synchronizing a Domain on a Destination CM Configuration Server from a Source CM Configuration Server that does not own the Domain. See Foreign-Owned Domain in this table.
Synchronization Pair	The two CM Configuration Servers that have been selected as the Source and Destination.
Domain Ownership	All Domains are “owned” by a CM Configuration Server. Domains are either **self-owned** or **foreign-owned**. See Domain Ownership on page 20.
Self-Owned Domain	A Domain that is owned by the current CM Configuration Server. **Note**: In order for a Domain to be self-owned, the owning MGR_ID and current MGR_ID must be identical.

Term	**Description**
Foreign-Owned Domain	A Domain that is owned by a CM Configuration Server other than the current one. **Note**: If the owning MGR_ID and current MGR_ID are different, the Domain is foreign-owned.
Unrelated Domains	Domains that are not owned by the same CM Configuration Server—that is, they do not have the same owning MGR_ID.
Middle-tier CM Configuration Server	A middle-tier CM Configuration Server is not an HP product. Rather this term is used exclusively to reference any CM Configuration Server on which the Source and Destination components are installed so that it can support peer synchronizations.
Container File	A file, created on the Source, in which the instance data is compressed before being transferred to the Destination. This file is much faster to transfer than a large number of small files. **Note**: At the Commit phase, the instance-container file is used as the data source, so the files are moved directly from it to their ultimate destination. This minimizes the number of times that the data is moved and the length of time that the CM Configuration Server Database is hard-locked.
edmprof file	This is the text file wherein the operational parameters of the CM Configuration Server are specified. • On UNIX platforms, this file is `.edmprof` • On Windows platforms, this file is `edmprof.dat`. **Note**: This guide uses this non-platform specific, generic reference.

2 Introduction to the CM Distributed Configuration Server

At the end of this chapter, you will have had the opportunity to learn:

- How the CM Distributed Configuration Server (CM-DCS) works to *synchronize HP OpenView Configuration Management Configuration Server Databases.*
- Why there are *two CM Distributed Configuration Server components*, and the *role of each* in ensuring a successful synchronization.
- How to define a pair of CM Configuration Servers for synchronization based on CM Configuration Server *eligibility* and *domain ownership.*
- The role of HP OpenView Configuration Management Configuration Server Database domains in CM Distributed Configuration Server operations, as well as: *domain-naming considerations*, *domain eligibility*, and *selecting domains.*
- How to establish *domain ownership across the enterprise*, and how to use this to set up *simultaneous synchronizations.*
- The *steps of the CM Distributed Configuration Server process*, which will aid in troubleshooting.

Overview

CM Distributed Configuration Server is a tool that enables an administrator to manage multiple CM Configuration Servers in a networked environment.

An administrator can use CM-DCS to replicate domains from one HP OpenView Configuration Management Configuration Server Database to another. This means that enterprise-wide changes can be made once, on one CM Configuration Server machine, then simply distributed to (replicated on) multiple down-line CM Configuration Servers within the enterprise. This ability offers several benefits:

- **Efficiency**
  Less time and manpower are required for making the database changes.
- **Reliability**
  Increased control over the integrity of the changes that are made.

CM Distributed Configuration Server

The CM-DCS product is a two-piece extension of the CM Configuration Server. The components—Source and Destination—function separate from, although in conjunction with, one another. Both, however, have some dependence on a CM Configuration Server, and therefore, each must be co-located with a CM Configuration Server.

Additional CM-DCS *dependency*, *directory,* and *requirement* information is presented in the section CM Distributed Configuration Server Directories starting on page 29.

For more information on the functionality of the CM-DCS components, see the section, CM Distributed Configuration Server Components starting on page 17.

In a multi-tier configuration, both components can be installed on the same machine in order to accommodate *peer synchronizations* via a *middle-tier CM Configuration Server*. (Peer synchronizations and middle-tier CM Configuration Servers are defined in Table 3 on page 13.)

CM-DCS is designed to synchronize CM-DCS-enabled CM Configuration Server Databases throughout an enterprise so, although it is not essential that the CM Configuration Server Databases directly communicate with one another, CM-DCS must be able to communicate with both CM Configuration

Servers that comprise the synchronization pair (see Two CM Configuration Servers: A Synchronization Pair on page 19).

In a synchronization operation, CM-DCS compares the control information of one CM Configuration Server Database with that of another, for the domains that have been selected.

CM Distributed Configuration Server Components

Inasmuch as there are two CM Configuration Servers involved in CM-DCS synchronizations, the two CM-DCS components perform different functions and must be installed separately, based on the intended role of the host CM Configuration Server.

- Each CM Configuration Server that will act as a Source must have the CM-DCS *Source* component installed.
- Similarly, each CM Configuration Server that will act as a Destination must have the CM-DCS *Destination* component installed.
- If a CM Configuration Server has both components of the CM-DCS installed, it can act as Source and Destination, albeit in separate CM-DCS operations.

With the CM-DCS components installed on the CM Configuration Server machines, CM-DCS:

- Provides the synchronization facilities to contact the Source and Destination,
- Reconciles the differences between the selected domains, and
- Provides the intermediate facilities to make identical the Source and Destination domains.

The Destination is always a replica of the Source.

The following section offers a more detailed look at these components and their functions.

Source vs. Destination

The Source and Destination components perform different functions during the CM Distributed Configuration Server synchronization. Therefore, it is important to correctly install these components in order to ensure: 1) the availability and accessibility of the appropriate Source-Destination synchronization pairs, and 2) the expected synchronization results.

Source Component

The Source component must be installed on any CM Configuration Server that is going to function as the master in a synchronization. This component contains the CM Integration Server (CM-IS), the product suite's HTTP server.

Integration Server Notes

- For a brief description of CM Integration Server and how it relates to CM-DCS, see CM Integration Server below.
- For a detailed description of CM Integration Server, refer to the *HP OpenView Configuration Management Essentials Guide (CM Essentials Guide*), available in the Configuration Management library.

The Source component loads the database instances into a single repository. This repository can be directly accessed, thereby eliminating the excessive overhead of opening, storing, transferring, and writing individual files for each CM Configuration Server Database instance.

CM Integration Server

CM Integration Server is the Configuration Management product suite's HTTP file server. It facilitates multiple concurrent file transfer sessions (HTTP "get" requests) and the creation of the instance-container file (see Container File in Table 3 starting on page 13).

CM Integration Server is not a separately licensed HP product. It integrates several independent modules—HP OpenView Configuration Management Portal (CM Portal) and HP OpenView Configuration Management Proxy Server (CM Proxy Server)—giving them access to all the functions and resources under its control.

Destination Component

The Destination component must be installed on any CM Configuration Server that is going to function as the target in CM-DCS synchronization. This component provides direct access to the target file system.

Two CM Configuration Servers: A Synchronization Pair

Two CM Configuration Servers, one defined as the Source and the other as the Destination, comprise a CM Distributed Configuration Server *synchronization pair*.

Cross-format synchronizations are not supported.

In order to be synchronized, the Source and Destination databases must be of the same format; that is, a **UTF-8** database to a **UTF-8** database, and a **Legacy** database to a **Legacy** database.

CM-DCS will accept one synchronization pair only, per execution. Operationally, because a synchronization can go in only one direction, this means that if two CM Configuration Servers (for example, MGR_001 and MGR_002) need domains from one another, two CM-DCS executions must be done—with MGR_001 being the Source in one synchronization, and MGR_002 being the Source in the other.

CM Configuration Server Eligibility

In order to be eligible to participate in a CM-DCS operation, a CM Configuration Server must meet the following requirements.

- In its `edmprof` file, it must be CM-DCS-enabled. This is done by specifying:

  ```
  [MGR_STARTUP]
  MANAGER_TYPE=DISTRIBUTED
  ```

  or

  ```
  [MGR_STARTUP]
  MANAGER_TYPE=SERVER
  ```

  All CM Configuration Servers are installed as DISTRIBUTED, so the SERVER value will have to be manually specified in the `edmprof` file.

  See Improving Performance using MANAGER_TYPE on page 20, for performance-improvement information.

- It must have either the CM-DCS Source or Destination component installed.

Improving Performance using MANAGER_TYPE

Typically, Destination and middle-tier CM Configuration Servers (see Middle-tier CM Configuration Server in Table 3 on page 14) get database updates only from their up-line Source CM Configuration Server. Therefore, some default database administrative processes are not necessary. HP indicates that disabling these unnecessary processes will improve performance.

- If a CM-DCS-enabled CM Configuration Server is going to be a Destination or middle-tier CM Configuration Server, and not managed via any other process, set:

  ```
  [MGR_STARTUP]
  MANAGER_TYPE=SERVER
  ```

Domain Ownership

HP OpenView Configuration Management Configuration Server Database (CM-CSDB) domains on each CM Configuration Server have three distinguishing characteristics: **domain name**, **owning MGR_ID**, and **current MGR_ID**. Their ownership is determined by the value of MGR_ID, and is established:

- When a CM-CSDB is installed, and
- When a domain is added to a CM-CSDB.

For planning purposes, HP recommends maintaining unique names for CM-CSDB domains.

- A self-owned domain is a CM-CSDB domain that is owned by the current CM Configuration Server.

  The owning MGR_ID and current MGR_ID are the same.

- A foreign-owned domain is a CM-CSDB domain that is owned by a CM Configuration Server other than the current one, and which is present as the result of a CM-DCS synchronization.

  The owning MGR_ID and current MGR_ID are not the same.

Domain Naming Considerations

To minimize the likelihood of synchronization problems, consider the following points when creating domain names and configuring synchronizations.

- A CM Configuration Server cannot contain two domains with the same name.
- A CM Configuration Server cannot obtain one of its self-owned domains from a CM Configuration Server that foreign-owns the domain. For example, MGR_001 cannot receive from another CM Configuration Server any domain for which it (MGR_001) is listed as the owning MGR_ID.

> The version that is resident at the owner is always considered the current and correct copy.
>
> Its contents will always supersede and replace any changes introduced by other CM Configuration Servers.

One Owner vs. Multiple Owners

When planning domain ownership, it is helpful to consider whether to assign the proprietorship of all the domains to one CM Configuration Server, thereby centralizing control; or to disperse control by establishing domain ownership at several CM Configuration Servers at various, strategic points across the enterprise.

The tables in this section detail the advantages and disadvantages of each method. For additional planning considerations, see CM Distributed Configuration Server Planning, starting on page 25.

One Owning CM Configuration Server

Table 4 lists the benefits and drawbacks of one CM Configuration Server owning all the domains.

Table 4 One domain-owning CM Configuration Server

Advantages	Disadvantages
Control of all applications, access rules, and users	Central control might make the database very large, depending on the organization and structure

Advantages	Disadvantages
One CM Configuration Server Database to backup	Does not align well with highly de-centralized organizations
Data flow throughout the environment is one-way	Data flow throughout CM-DCS is one-way
Aligns with highly centralized organizations	

Multiple Owning CM Configuration Servers

Table 5 lists the benefits and drawbacks of domain ownership being assigned to multiple CM Configuration Servers.

Table 5 Multiple domain-owning CM Configuration Servers

Advantages	Disadvantages
Aligns readily with highly de-centralized organizations	Does not align well with highly centralized organizations
Databases are smaller and indicative of regional Source CM Configuration Servers	Multiple CM Configuration Servers must be administered and backed-up
Applications and users can be managed locally	Allows for two-way data flow, adding complexity to the CM-DCS design
Corporate or common information can be managed centrally, while local information is managed locally	
Allows for two-way data flow between central and local CM Configuration Servers	

Any CM Configuration Server with self-owned domains should be backed up.

Foreign-owned domains can always be obtained through synchronization with the owning CM Configuration Server.

Domain Eligibility

The list of domains that are eligible for synchronization is dynamically compiled by CM Distributed Configuration Server. This list is based on the chosen synchronization pair and:

- The database control information concerning the most recent synchronization for the synchronization pair, or
- The most recent update with Configuration Management administrative components (such as CM Administrator Configuration Server Database Editor, CM Administrator Packager, and CM Administrator Publisher).

Only domains that have the same owner (on the Source and Destination) can be synchronized between that pair of CM Configuration Servers.

Selecting Domains

It is not necessary to synchronize all eligible domains between two CM-DCS-enabled CM Configuration Servers. At the start of each session, an administrator can specify which of the eligible domains are to be synchronized.

Domain Eligibility Rules

The primary CM-DCS domain synchronization eligibility rules are listed below. These apply to each domain independently. See Log Error Messages on page 60.

- Synchronization cannot occur into a self-owned domain.
- There is no replication into an owning CM Configuration Server.

  If a self-owned domain is deleted, it must be restored from a backup; it cannot be replicated from a CM-DCS-enabled CM Configuration Server on which it is foreign-owned.

- Domains that are not owned by the same CM Configuration Server are considered *unrelated*. A domain must be owned by the same MGR_ID at the Source and Destination in order to be eligible for synchronization.
- Once a foreign-owned domain is locally updated with another Configuration Management component, it cannot be used as the Source in a *peer synchronization*.

➤ A local update occurs when a database is updated via a Configuration Management component (such as CM Admin CSDB Editor, CM Admin Publisher, and CM Admin Packager) other than CM Distributed Configuration Server.

- When it is possible to make such a distinction, the CM-DCS will prevent the regression of a more current Destination by a less current peer Source. If the Destination domain has been locally updated, and the relative currency cannot be determined, the synchronization is allowed.

CM Distributed Configuration Server Configuration

CM Distributed Configuration Server functionality must be configured for two CM Configuration Servers.

CM-DCS requires a communications connection between the Source and Destination CM Configuration Servers.

CM Distributed Configuration Server: Batch Mode

The command-line mode (also known as the **batch** mode) of CM-DCS is invoked by the executable, `DMABATCH.EXE`. Once the synchronization is started, it will execute with no administrator action required. This is discussed in more detail in CM Distributed Configuration Server Options and DMABATCH, on page 47.

Synchronization Logs

When a synchronization is executed, logs and objects are created. Each subsequent run causes its predecessor's logs to be overwritten, so that these logs and objects represent the most recent CM-DCS synchronization.

Simultaneous Synchronizations

A CM Configuration Server can be simultaneously involved in multiple synchronizations in which it is the Source only. This is possible because a Source database is only being read from, whereas a Destination database is being written to.

- A CM Configuration Server cannot simultaneously be a Source and Destination for different synchronizations.
- A CM Configuration Server cannot be the Destination in multiple, simultaneous synchronizations.

CM Distributed Configuration Server Planning

This section offers planning considerations when CM Distributed Configuration Server is being implemented within a CM Configuration Server environment.

When to Use CM Distributed Configuration Server

The following is a list of situations that might arise in a software management enterprise, and in which the capabilities of CM-DCS would prove beneficial.

- To replicate CM Configuration Server Database contents across an enterprise.
- When moving domains from a test environment to a production environment.
- As an alternative to local connects.

Developing a viable, functional CM-DCS infrastructure requires knowledge of:

- The Configuration Management resolution process within an environment,
- The hardware and communications configuration of an environment, and
- The Configuration Management-managed information within an infrastructure.

3 Installing the CM Distributed Configuration Server

At the end of this chapter, you will have had the opportunity to:

- Install the CM Distributed Configuration Server (CM-DCS) **Source** component.
- Install the CM Distributed Configuration Server **Destination** component.

Two-Phase Installation

In order set up a distributed CM Configuration Server synchronization environment, CM Distributed Configuration Server enables a Configuration Management (CM) administrator to install:

- The CM-DCS Source component,
- The CM-DCS Destination component, or
- Both CM-DCS components.

The installations are outlined in Installing the CM Distributed Configuration Server, starting on page 30.

- The CM-DCS **Source** component must be installed on any CM Configuration Server whose database is going to be the **master** in CM-DCS synchronization.
- The CM-DCS **Destination** component must be installed on any CM Configuration Server that is going to be the **target** (also referred to as **slave**) in CM-DCS synchronization.

A CM Configuration Server can have both components installed, in which case it can function as Source and Destination in separate CM-DCS operations.

For a detailed description of these components, see Source Component and Destination Component on page 18.

System Requirements

To ensure the successful installation and operation of CM Distributed Configuration Server, the following system requirements are recommended.

- Communications protocol: **TCP/IP** only.
- Pentium processor (minimum): **120 MHz**.

Platform Support

Both components of CM Distributed Configuration Server are dependent on, and must be co-resident with, a CM Configuration Server.

For information about the platforms that are supported in this release, see the accompanying release notes.

CM Distributed Configuration Server Directories

This section details (by platform) the directories that are created by default by the installations of the CM Distributed Configuration Server components.

Source

If this is the initial installation of the CM Distributed Configuration Server Source component (meaning there is *not* an existing CM Integration Server element), the following directories are created by default.

- Windows

  `SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer` and its subdirectories

- UNIX

  `/opt/HP/CM/IntegrationServer` and its subdirectories

If there is an existing CM Integration Server element, no directories are added by the installation; however, the first execution of the CM-DCS execution will add `IntegrationServer_directory\data\dcs`.

Destination

If this is the initial installation of the CM Distributed Configuration Server Destination component, the following directories are created by default.

- Windows

  `SystemDrive:\Program Files\Hewlett-Packard\CM\dcs`

  `SystemDrive:\Program Files\Hewlett-Packard\CM\dcs\lib`

  `SystemDrive:\Program Files\Hewlett-Packard\CM\dcs\log`

  `SystemDrive:\Program Files\Hewlett-Packard\CM\dcs\master*`

  `SystemDrive:\Program Files\Hewlett-Packard\CM\dcs\slave*`

  `SystemDrive:\Program Files\Hewlett-Packard\CM\lib`

- UNIX

```
/opt/HP/CM/dcs
/opt/HP/CM/dcs/lib
/opt/HP/CM/dcs/log
/opt/HP/CM/dcs/master*
/opt/HP/CM/dcs/slave*
/opt/HP/CM/lib
```

If there is an existing installation of CM-DCS, the parameter, IDMASYS, is added to the `nvd.ini` file in the following existing directories.

- Windows

  SystemDrive:\Program Files\Hewlett-Packard\CM\lib

- UNIX

  /opt/HP/CM/lib

CM Distributed Configuration Server Space Requirements

The amount of free disk space that is required by the CM Distributed Configuration Server components will vary because it is dependent on the number of domains that are selected, their size, which domains are selected, and the size of the synchronization differences.

Installing the CM Distributed Configuration Server

This section details the installation of the CM Distributed Configuration Server. In the exercise that follows, the Source and Destination component installations were selected.

Although this exercise is performed in a Windows environment, the UNIX steps are similar, but with the expected platform differences. Additionally, there are pre-installation steps for a UNIX environment, which are described in the section, UNIX Pre-Installation Notes, starting below.

UNIX Pre-Installation Notes

Make sure that the user that is performing the installation has:

- Adequate UNIX operating system rights in order to create and update the target installation directory.
- A `home` directory on the UNIX workstation, and is logged in as **root**.

To install the CM Distributed Configuration Server

1. Insert the installation media and in the `extended_infrastructure` directory, navigate to the `distributed_configuration_server` installation files.
2. Double-click **setup.exe**.

   The CM Distributed Configuration Server Install Welcome window opens.
3. Click **Next**.

   The CM Distributed Configuration Server Install HP Software Licensing Agreement window opens.
4. Click **Accept**.

   If **Accept** is not selected, the installation program will terminate.

   The CM Distributed Configuration Server Installation Component Selection window opens.

   — Select either, or both, of the CM Distributed Configuration Server components.
5. Click **Next**.

   The CM Distributed Configuration Server Installation Summary window opens. It displays the CM Distributed Configuration Server components that will be installed.

   — To change the selections, click **Back** and make the necessary changes.
6. To install the displayed components, click **Install**.

   The standard "transferring files" window will display. After a brief interval, the CM Distributed Configuration Server (Source) Install Welcome window will appear.

Installing the CM Distributed Configuration Server Source Component

This section describes the installation of the Source component of CM Distributed Configuration Server.

The CM Distributed Configuration Server (Source) Install Welcome window opens.

1 Click **Next**.

   The CM Distributed Configuration Server (Source) Install HP Software License Agreement window opens.

2 Click **Accept**.

   If **Accept** is not selected, the installation program will terminate.

   The CM Distributed Configuration Server (Source) Install File Location window opens.

   In the CM Distributed Configuration Server (Source) Install File Location window, only ASCII characters are supported for the installation directory setting.

   The CM Distributed Configuration Server (Source) field displays the directory in which the CM Distributed Configuration Server Source component's files will be installed.

   - If the installation program detects an existing Configuration Management element (such as a CM agent, CM Administrator, or a previous version of CM Distributed Configuration Server), the window will have one field—for the installation location.

     The existing object and log locations, specified by IDMROOT and IDMLOG will continue to be used, unchanged.

   - If the installation program detects no existing Configuration Management element, the window will have Object Location and Log Location fields under the Installation Location field.

   In either case, a message will appear, warning that the directory will be updated.

   Click **OK** to proceed and allow the update, or click **Cancel** to return to the Installation Location window and specify a different directory.

— Accept the default path that is displayed (*recommended*); or

— Specify a different location by typing it in the field or clicking **Browse** and navigating to it.

3 Click **Next**.

The CM Distributed Configuration Server (Source) Install Database Path window opens.

The Source CM-CS Database Path field displays the directory in which the CM Configuration Server Database was installed.

— Accept the path that is displayed (*recommended*); or

— Specify a different location by typing it in the field or clicking **Browse** and navigating to it.

4 Click **Next**.

The CM Distributed Configuration Server (Source) Install Summary window opens. This window displays the directory into which the CM Distributed Configuration Server Source component will be installed.

— To change the selections, click **Back** and make the necessary changes.

5 To accept the specified settings, click **Install**.

The CM Distributed Configuration Server (Source) Install Finish window opens.

6 Click **Finish**.

The Source component of CM Distributed Configuration Server has successfully installed.

➤ If the installation of the CM Distributed Configuration Server Destination component was also selected, it will automatically start now.

Installing the CM Distributed Configuration Server Destination Component

This section describes the installation of the Destination component of CM Distributed Configuration Server.

The CM Distributed Configuration Server (Destination) Install Welcome window appears.

1 Click **Next**.

The CM Distributed Configuration Server (Destination) Install HP Software License Agreement window opens.

2 Click **Accept**.

> ➤ If **Accept** is not selected, the installation program will terminate.

The CM Distributed Configuration Server (Destination) Install Installation Location window opens.

> ➤ In the CM Distributed Configuration Server (Destination) Install File Location window, only ASCII characters are supported for the installation location setting.

The Installation Location field displays the directory into which the CM Distributed Configuration Server Destination component's files will be installed.

- If the installation program detects any existing Configuration Management element (such as a CM agent, CM Administrator, or a previous version of CM Distributed Configuration Server), the window will have one text field—for the installation location.

  The existing object and log locations, specified by IDMROOT and IDMLOG will continue to be used, unchanged.

- If the installation program detects no existing Configuration Management element, the window will have Object Location and Log Location fields under the Installation Location field.

> ➤ In either case, a message will appear, warning that the directory will be updated.
>
> Click **OK** to proceed and allow the update, or click **Cancel** to return to the Installation Location window and specify a different directory.

— Accept the default path that is displayed (*recommended*); or

— Specify a different location by typing it in the field or clicking **Browse** and navigating to it.

3 Click **Next**.

If a CM Configuration Server is installed on this machine, the information for the next three windows (Local CM Configuration Server ID and Local CM Configuration Server Ports [TCP/IP and SSL]) will be read from the `edmprof` file of the CM Configuration Server, and these windows will not appear during this installation.

Continue with step 4 below.

If a CM Configuration Server is *not* installed on this machine (or, optionally, on Windows, IS installed, but IS NOT running as a Windows service), specify the information this is requested.

a In the CM Distributed Configuration Server (Destination) Install Local CM Configuration Server ID window, specify a valid 3-character, hexadecimal CM Configuration Server ID, and click **Next**.

  Valid values are within the hexadecimal (0-9 and A-F) range of **001** to **EFF**.

b In the CM Distributed Configuration Server (Destination) Install Local CM Configuration Server TCP/IP Port window, specify as 3–5 decimal digits, and click **Next**.

c In the CM Distributed Configuration Server (Destination) Install Local CM Configuration Server SSL Port window, specify as 3–5 decimal digits, and click **Next**.

4 Click **Next**.

The CM Distributed Configuration Server (Destination) Install Source CM Configuration Server Host Address window opens.

> This series of windows enables an administrator to configure a default *synchronization pair*—of Source and Destination CM Configuration Servers.

The Source CM Configuration Server Host Address field is where the IP address of the Source CM Configuration Server is specified.

- Specify the IP address of the Source CM Configuration Server in the standard internet dotted-decimal format (*`11.111.222.111`*); or
- In the symbolic format (*`myhost.mycorp.net`*).

5 Click **Next**.

The CM Distributed Configuration Server (Destination) Install Source CM Configuration Server ID window opens.

In this window, specify the ID (MGR_ID) that was assigned during the installation of the Source CM Configuration Server whose IP address was specified in the previous window.

- Specify a valid 3-character, hexadecimal CM Configuration Server ID.

Valid values are within the hexadecimal (0-9 and A-F) range of **001** to **EFF**.

The installation will accept any valid 3-character, hexadecimal CM Configuration Server ID value, as described above.

It is important that the administrator who is conducting this installation is sure that this is the ID that is assigned to the CM Configuration Server that was designated in the previous step; the installation will not perform any type of CM Configuration Server ID verification in the environment.

6 Click **Next**.

The CM Distributed Configuration Server (Destination) Install Source CM Configuration Server TCP/IP Port window opens.

In this window, specify the TCP/IP port of the Source CM Configuration Server whose ID was specified in the previous window.

The default CM Configuration Server port, **3464**, is displayed when this window opens. If this default was changed when the CM Configuration Server was installed, be sure to specify the correct port.

— Accept the default CM Configuration Server TCP/IP port that is displayed, **3464**, (*recommended*); or

— Specify a valid 3- to 5-character decimal CM Configuration Server TCP/IP port.

7 Click **Next**.

The CM Distributed Configuration Server (Destination) Install Source CM Configuration Server SSL Port window opens.

In this window, specify the SSL port of the Source CM Configuration Server from the previous window.

— Accept the default CM Configuration Server SSL port that is displayed, **443**, (*recommended*); or

— Specify a valid 3- to 5-character decimal CM Configuration Server SSL port.

8 Click **Next**.

The CM Distributed Configuration Server (Destination) Install CM Integration Server TCP/IP Port window opens.

In this window, specify the TCP/IP port of the CM Integration Server.

— Accept the default CM Integration Server TCP/IP port that is displayed, **3466**, (*recommended*); or

— Specify a valid 3- to 5-character decimal CM Integration Server TCP/IP port.

9 Click **Next**.

The CM Distributed Configuration Server (Destination) Install CM Integration Server SSL Port window opens.

In this window, specify the SSL port of the CM Integration Server.

— Accept the default CM Configuration Server SSL port that is displayed, **444**, (*recommended*); or

— Specify a valid 3- to 5-character decimal CM Configuration Server SSL port.

10 Click **Next**.

The CM Distributed Configuration Server (Destination) Install Domains window opens.

In this window, specify the domains that will be included in synchronizations between this (Destination) CM Configuration Server and the Source CM Configuration Server that has been defined in the previous windows.

— To include all eligible domains, leave the Domain(s) field blank.

— To include multiple domains, specify the domain names separated by a space.

11 Click **Next**.

The CM Distributed Configuration Server (Destination) Install Enable SSL for window opens.

In this window, specify whether SSL should be enabled for the CM Integration Server and the Source *and* Destination CM Distributed Configuration Servers.

— Click **Enable** or **Disable**.

> If you enable SSL, the CM Integration Server and CM Configuration Servers must be configured for SSL.

12 Click **Next**.

The CM Distributed Configuration Server (Destination) Install Credentials window opens.

In this window, specify credentials that can be used with any CM Configuration Server and any CM Integration Server that requires authentication.

13 Click **Next**.

The CM Distributed Configuration Server (Destination) Install Summary window opens. This window displays the directory into which the CM Distributed Configuration Server Destination component will be installed.

— To change the selections, click **Back** and make the necessary changes.

14 To accept the specified settings, click **Install**.

The CM Distributed Configuration Server (Destination) Install Finish window opens.

15 Click **Finish**.

The Destination component of CM Distributed Configuration Server has successfully installed.

The CM Distributed Configuration Server Install Finish window opens.

16 Click **Finish**.

Both components of CM Distributed Configuration Server have been successfully installed.

Windows

- This installation might create a new (or update an existing) `nvd.ini` file in `C:\Program Files\Hewlett-Packard\CM\lib`.
- If there was an `nvd.ini` file under `C:\Program Files\Hewlett-Packard\CM\lib`, it gets renamed to `nvd.ini.old`.

UNIX

- This installation might create a new (or update an existing) `~/.edmprof`.
- If there was an `.edmprof` file, it gets renamed to `.edmprof.old`.

Post-installation Notes

The associated CM-DCS log file and objects will be created in the directories that are specified by the IDMLOG and IDMLIB variables, respectively, or the default directory for CM-DCS. The log file is `DMABATCH.LOG`.

> The values of the IDMLIB and IDMLOG variables can be overridden by the `-libpath` and `-logpath` options in the CM-DCS configuration file, `dmabatch.rc`.

Setting a Temporary Directory

For each of the CM Distributed Configuration Server components, it is possible to override the default location that is used to save temporary files. This is beneficial in situations where there are policy constraints on where new files can be created.

There are two customizations, one each for the Source and Destination.

Source Component

By default, the Source component's temporary files are created in a subdirectory of the CM Integration Server's root directory. Using the `TMPDIR` parameter in the `/etc/dcs.cfg` configuration file, specify a different location, for example:

```
dcs::init {
   TMPDIR c:/rdcs-source
   DBPATH c:/Program Files/Hewlett-Packard/CM
          /Configuration Server/db
}
```

Save and close the configuration file and restart the CM Integration Server.

Destination Component

By default, the Destination component's temporary files are created in a subdirectory of the CM Distributed Configuration Server's root directory. Using the parameter `-temp-dir` in the `dmabatch.rc` configuration file, specify a different location, for example:

```
array set O {
  -temp-dir      c:/rdcs-dest
  -http-host     ""
  -http-port     3466
}
```

All Platforms

A slash (/) must be used as the directory separator for the parameter, **`-temp-dir`**.

Save and close the configuration file and restart the CM Configuration Server.

4 The EDMPROF File and CM DCS Security

At the end of this chapter, you will have had the opportunity to:

- Review the CM Configuration Server *edmprof file* sections and settings that are relevant to CM Distributed Configuration Server operations.
- Set up *password protection* for CM Distributed Configuration Server synchronizations.

The EDMPROF File

The edmprof file is the text file in which the operational parameters of the CM Configuration Server are configured and stored. Two of its sections—**MGR_STARTUP** and **MGR_DMA**—are integral to enabling CM-DCS and ensuring its proper operation.

Information on these edmprof sections, including their settings, acceptable values, and impact on CM-DCS processing is presented in this section.

For a comprehensive look at the edmprof file, refer to the *HP OpenView Configuration Management Configuration Server User Guide* (*CM Configuration Server Guide*).

MGR_STARTUP Section

The MGR_STARTUP section dictates startup behavior for the CM Configuration Server. The following MGR_STARTUP settings are essential to the operation of the CM-DCS.

Table 6 MGR_STARTUP Settings and Values

Setting	Explanation
MANAGER_TYPE	STANDALONE is the default value that is established when the CM Configuration Server is installed. In order to ensure that a CM Configuration Server is CM-DCS-enabled, change this value to either **SERVER** or **DISTRIBUTED**. For additional information, see CM Configuration Server Eligibility on page 19.
MGR_NAME	A 32-alphanumeric character (max.) CM Configuration Server identifier.
MGR_ID	The unique, 3-digit, hexadecimal ID for a CM Configuration Server. For more information, see MGR_ID, on page 43. • CM-DCS uses this value to generate object IDs in the CM-CSDB. • Each character in this identifier can have the values 0-9 and A-F. **Exception**: The 256 consecutive positions from F00 through FFF are reserved for use with Configuration Management.

Setting	Explanation
TCP_PORT	The port on which the CM Configuration Server will listen. This must match the port that is specified for CM-DCS communications (`-master-port` in `dmabatch.rc`).

MGR_ID

The MGR_ID setting establishes a unique identity for each CM Configuration Server. All Domains in a CM Configuration Server Database (CM-CSDB) are *owned* by a CM Configuration Server—identified by the value of MGR_ID.

It is possible that a Domain is not owned by the CM Configuration Server that is hosting its database.

CM-DCS uses the value of MGR_ID to determine which CM Configuration Server owns each Domain.

Domain ownership is important because in order for a Domain to be eligible for synchronization its owning MGR_ID must be the same on the Source and Destination CM Configuration Servers. If the owning MGR_IDs do not match, synchronization cannot occur.

Although the MGR_ID must match for both Domains, it is possible that neither the Source nor the Destination is the owner. See Foreign-Owned Domain, in Table 3 on page 13.

MGR_DMA Section

In addition to the MGR_DMA settings that are needed to establish CM-DCS password protection (described in CM Configuration Server Security Settings on page 44), there is another CM-DCS-related setting, DMA_TIMEOUT, which is detailed in Table 7 below.

Table 7 MGR_DMA Settings and Values

Setting	Explanation of Value
SECURITY_ METHOD	Optional. If not specified, security verification is disabled. To enable native operating system security, specify **`EDMSIGN`**.
ADMIN_LIST	This setting is required if a SECURITY_METHOD is specified. Specify the list of administrators (user IDs) that are allowed to use CM-DCS on this CM-CSDB. The format is a comma-separated (no spaces), case-sensitive list of operating system account names.

Setting	Explanation of Value
DMA_TIMEOUT	Specify the number of seconds that CM-DCS is to wait for non-CM-DCS tasks to complete before applying a lock to the CM Configuration Server Database. If CM-DCS times out before the task ends, it will abort. The default is **0**. • When soft-locking the CM-CSDB, CM-DCS must wait for all administrator tasks to end. • When hard-locking the CM-CSDB, CM-DCS waits for all non-CM-DCS tasks to end.

Setting up Security

CM Distributed Configuration Server (CM-DCS) has an optional security feature that enables an administrator to assign password protection to one or both of the synchronization pair's CM Configuration Server Databases (CM-CSDB), using native operating system security.

Native Operating-System Security

This section details the assignment of password protection to the native operating system.

A special user ID and password are used to access secured CM-CSDBs. CM-DCS defines only one user ID and password. Therefore, all secured CM-CSDBs that CM-DCS might access must:

- Be defined in the `edmprof` files of their host's security system,
- Have the user ID in the ADMIN_LIST section of their `edmprof` files, and
- Have the same password for that user ID.

The user ID and password values are defined in the `-userid` and `-password` options of the configuration file.

CM Configuration Server Security Settings

In addition to the steps outlined in Native Operating-System Security, the MGR_DMA section must be added to the `edmprof` file, as described in this section.

The MGR_DMA section is not included in the edmprof file after the CM Configuration Server installation because it is not needed for default operations.

It can be added to the edmprof file in order to configure CM-DCS as a default function of the CM Configuration Server.

To modify the edmprof file

1 Stop the CM Configuration Server.

2 Open the edmprof file using a text editor.

3 Add the section, MGR_DMA, and the settings shown below:

```
[MGR_DMA]
SECURITY_METHOD = EDMSIGNR
ADMIN_LIST = list_of_administrators
```

For a description of these settings, see Table 7 on page 43.

4 Save the changes, close the edmprof file, and restart the CM Configuration Server.

The administrators that are specified for ADMIN_LIST must have user rights under local policy settings on the host operating system.

For information on establishing operating system-specific user rights and policies, consult the operating system's product documentation.

5 CM Distributed Configuration Server Options and DMABATCH

At the end of this chapter, you will have had the opportunity to learn more about:

- The CM Distributed Configuration Server configuration file, `dmabatch.rc`.
- The DMABATCH synchronization message variable, BATCHMSG, and the return-code variable, BATCHRC.
- The DMABATCH command-line arguments that can be used in a script.

CM Distributed Configuration Server Configuration File

In this section, Table 8, details the options that are in the CM Distributed Configuration Server configuration file, `dmabatch.rc`. These options can be edited by opening `dmabatch.rc` in a text editor.

- All of the options that are important to the basic operation of CM-DCS are populated by values that were specified during the CM-DCS Source and Destination installation programs (see the 3rd column, Set by Install, in Table 8)
- Only occasionally will any of the options need to be manually modified; that is when a non-default value is preferred.

Terminology

In Table 8, the following CM Distributed Configuration Server terminology is used.

- CM-IS = CM Integration Server
- Master = the Source CM Configuration Server
- Slave = the Destination CM Configuration Server

Table 8 dmabatch.rc options

Option	Default Value or Required	Set by Install	Description
-master-host	Required	Y	IP name/address of the master CM-CS
-master-id	Required	Y	3 hexadecimal-digit ID of the master CM-CS
-master-port	Required	Y	TCP port of the master CM-CS (usually 3464)
-master-ssl-port	443	Y	SSL port of the master CM-CS (usually 443)
-master-timeout	3600	Y	Master CM-CS request timeout (in seconds)

Option	Default Value or Required	Set by Install	Description
-slave-host	Required	Y	IP name/address of the slave CM-CS (local computer name or *localhost*)
-slave-id	Required	Y	3 hexadecimal-digit ID of the slave CM-CS
-slave-port	Required	Y	TCP port of the slave CM-CS (usually 3464)
-slave-ssl-port	443	Y	SSL port of the slave CM-CS (usually 443)
-slave-timeout	3600	Y	Slave CM-CS request timeout (in seconds)
-http-port	3466	Y	TCP port of the CM-IS (usually 3466)
-https-port	444	Y	SSL port of the CM-IS (often 444; must not be the same as that of `-master-ssl-port`)
-domains	“ ” (null)	Y	Quoted list of blank-separated CM-CSDB Domains; null list means “ALL DOMAINS”
-ssl	0	Y	Enable SSL? 1=enable; 0=disable
-userid	DMABATCH	Y	User ID to be used for CM-CS and/or CM-IS authentication
-password_cipher	AES	Y	TP password-encryption method: AES or DES
-password	<none>	Y	Password to be used for CM-CS and/or CM-IS authentication **Note**: This value can be AES-encrypted or cleartext.
-loglvl	3	Y	Logging level: 3=normal, 4=debug, 5=debug+
-logfile	`dmabatch.log`	N	Log file name (no pathing)
-logmode	w	N	Overwrite the log file? w=overwrite; a=append the log file

Option	Default Value or Required	Set by Install	Description
-loglines	100000	Y	Number of lines to write to the log file before the log rolls over
-logerr	1	Y	Echo log to `stderr`? 1=echo; 0=don’t echo
-logpath	<none>	N	Override LOGPATH in `nvd.ini` (location of `dmabatch.log`)?
-libpath	<none>	N	Override LIBPATH in `nvd.ini` (location of client objects)?
-commit	1	N	Commit database updates? 1=commit; 0=don’t commit, but remain locked See also Deferred Commit on page 55.
-report	0	N	Send status-reporting objects to master CM-CS? 1=send; 0=don’t send
-dmastats-userid	DMA_<id>_ <id>_<domains>	N	Value of ZUSERID in reporting object, when `-report 1`. **Note**: For use with CM-CS method, ZPUTPROF.
-reset	0	N	Reset state and unlock CM-CSs on error? 1=reset; 0=leave locked on error
-lock-to	FAIL	N	Action on pending hard-lock timeout: FAIL, RETRY, or FORCE? **Note**: FORCE = kill all non-CM-DCS tasks on slave CM-CS.

Configuration Object Equivalents

Some of the options in `dmabatch.rc` have operational equivalents in the configuration objects `ZMANAGER` and `ZMGRSYNC`. Table 9, on page 51, lists these equivalents.

Table 9 Configuration object equivalents of dmabatch.rc options

Option	Set by Install	Configuration Object Equivalent
`-master-host`	Y	ZMANAGER.ZTCPADDR
`-master-id`	Y	ZMGRSYNC.ZSRCMGID
`-master-port`	Y	ZMANAGER.ZTCPPORT
`-master-timeout`	Y	ZMANAGER.ZTIMEO
`-slave-host`	Y	ZMANAGER.ZTCPADDR
`-slave-id`	Y	ZMGRSYNC.ZDSTMGID
`-slave-port`	Y	ZMANAGER.ZTCPPORT
`-slave-timeout`	Y	ZMANAGER.ZTIMEO
`-domains`	Y	ZMGRSYNC.ZDOMAINS
`-userid`	Y	ZMGRSYNC.BATUSER
`-password`	Y	ZMGRSYNC.BATPWD
`-report`	N	ZMGRSYNC.REPORT
`-dmastats-userid`	N	ZMGRSYNC.REPTNAME
`-reset`	N	ZMGRSYNC.BATRESET
`-lock-to`	N	ZMGRSYNC.BATLOKTO

Using PUTPROF

1 In SYSTEM.PROCESS create a new instance, such as DMASTATS.

- Specify the **Method** attribute as:

  `SYSTEM.ZMETHOD.PUTPROF_DMASTATS`

2 In SYSTEM.ZMETHOD create a new instance, such as PUTPROF_DMASTATS.

- Specify the **Parameter** attribute as **`DMASTATS`**
- Specify the **Method Name** attribute as **`EDMMPPRO`**

➤ Each execution of CM-DCS might generate several reporting objects at various points in the processing (see DMASTATS below). Each of these reporting objects will overwrite the previous one.

DMASTATS

Table 10 defines the fields of the DMASTATS object.

Table 10 DMASTATS fields defined

Field	Definition
BATCHDAT	Date of this report
BATCHTIM	Time of this report
BATSTDAT	Date of correlated starting (id=1) report
BATSTTIM	Time of correlated starting (id=1) report
BATCHRC	Character return code (if REPORTID > 1) **Notes**: See Table 11 on page 53 for REPORTID values. See Table 12 on page 53 for detailed BATCHRC information.
BATCHMSG	Completion message (if REPORTID > 1) **Note**: See Table 11 on page 53 for REPORTID values.
BATARGS	DMABATCH command line
BATLKSTA	Result of **`DMABATCH ACTION=LOCKSTATUS`**: **U** (Unlocked); **S** (Soft-locked); **X** (Exclusive Soft-locked); **H** (Hard-locked)
DMASTATE	**0** = Initial; **1** = Compared; **2** = Downloaded; **3** = Committed
ZSRCMGID	`-master-id` (Source MGR_ID)
ZDSTMGID	`-slave-id` (Destination MGR_ID)
REPORTID	Identifies which CM-DCS processing point sent the report. **Note**: See Table 11 on page 53 for detailed REPORTID information.
SCOPE	N/A
ZDOMAINS	List of domains
ZUSERID	User name for use with PUTPROF method (see ZUSERID on page 53)

Table 11 identifies which DMASTATS.REPORTID processing point sent the report.

Table 11 REPORTID values defined

REPORTID	Definition
1	Starting
2	Differencing completed, differences found
3	Differencing completed, no differences found
4	Staging completed
5	Commit completed
6	Ending

Every DMABATCH execution sends REPORTIDs 1 and 6. In addition, synchronizations might send REPORTIDs 3 or 2, 4, and 5 for intermediate status.

Table 12 lists the CM Configuration Server BATCHRC and corresponding BATCHMSG responses to CM Distributed Configuration Server requests.

Table 12 BATCHRC and BATCHMSG values

BATCHRC	BATCHMSG
000	No differences found. / Successfully Completed
001	dmabatch internal structural error
016	Execution failed (see BATCHMSG for details).
101	Invalid cmdline keyword or keyword combination; master & slave IDs same.
103	CM-CS ID/host/port not specified (see BATCHMSG for details).
108	No eligible domains.

ZUSERID

If `-dmatstats-userid` was specified in the configuration file (`dmabatch.rc`), ZUSERID uses that value. This name can be:

- A 32-character (maximum) alphanumeric name.

  If it is longer than 32 characters, it will be truncated.

- US national characters, such as **@**, **$**, **#**, and _ are allowed.

If `-dmatstats-userid` was not specified in the configuration file (`dmabatch.rc`), ZUSERID is generated based on one of the following.

- If a synchronization operation:

  ```
  DMA_src-id_dest-id_DOMS_domains
  ```

  where *`domains`* is an underscore-separated list of Domains in this synchronization, or ALL if ZDOMAINS=*. For example,

  ```
  DMA_100_203_DOMS_SOFTWARE_POLICY
  ```

- If a special stand-alone operation (such as ACTION=LOCK):

  ```
  DMA_<target_id>_<action>
  ```

  ```
  DMABATCH ACTION=LOCKSTATUS MGRID=123
  ```

  generates

  ```
  DMA_123_LOCKSTATUS
  ```

  `target_id` can be independent of *`src_id`* and *`dst_id`*.

DMABATCH Command-line Options

Reset

Normally, if synchronization fails during the Staging phase (for example, due to a lost connection), it is left in a state that ensures that it can subsequently be restarted from the point of failure. This entails leaving both CM Configuration Servers locked. If leaving both CM Configuration Servers locked, pending a restart, is not acceptable, this option allows the session to be reset to the initial state.

- To manually reset a failed session, specify:

  ```
  DMABATCH ACTION=RESET
  ```

This action causes an immediate unlocking of both CM Configuration Servers; staged resources will immediately be freed. The trade-off is that “restartability” is sacrificed, which can be a problem if staging failed near the end of a long process.

Deferred Commit

CM-DCS offers the ability to defer committing the database updates on the Destination CM Configuration Server to a time when it is less busy. To do this, use the DMABATCH command, COMMIT, as shown below.

- To defer the "commit" to a time when the Destination CM Configuration Server is less busy, specify:

  `DMABATCH COMMIT=NO`

  All CM-DCS processing will be halted after the Staging phase.

This command is equivalent to `-commit 0` in `dmabatch.rc`.

If Staging is successful, `BATCHRC=000` and the following message will be returned,

```
ZMGRSYNC.BATCHMSG="Commit bypassed by COMMIT=NO"
```

At this point the:

- Source CM Configuration Server will be unlocked,
- Destination CM Configuration Server will be soft-locked.

To commit the database updates to the Destination CM Configuration Server, the Commit phase must subsequently be done without **`COMMIT=NO`**.

DMABATCH Scripting Commands

The functions that are described in this section are DMABATCH command-line arguments, intended for use in a script that executes DMABATCH and handles error conditions. These functions are called with the command,

`DMABATCH ACTION=`

If no value is specified for **`ACTION`** (as seen above), or if **`ACTION=SYNC`**, a normal synchronization is done.

Any other **`ACTION`** value does the indicated action only, with no synchronization.

DMABATCH Line Commands

This section details the use and functionality of the DMABATCH commands.

DMABATCH ACTION=QUIESCE [CSID=*id*][QTYPE=TASK|TRANS]

This command quiesces the Destination, thereby increasing the chance of later obtaining a hard-lock.

- If **`CSID=`** is omitted, the default is the Destination's ID.
- **`QTYPE=TASK`**: prevents any new, non-CM-DCS CM agent tasks from starting.
- **`QTYPE=TRANS`**: same as TASK, but also, for currently running non-CM-DCS CM agent tasks, the CM agent connection terminates when the CM agent sends the next transaction.
- This action would likely be scripted to run before a synchronization, thereby decreasing the likelihood of later having to stop any tasks.

DMABATCH ACTION=RESUME [CSID=*id*]

This command ends a "quiescent" state on the Destination.

- If **`CSID=`** is omitted, the default is the Destination's ID.

DMABATCH ACTION=KILLTASKS [CSID=*id*]

This command should be used if QUIESCE was not sufficient to clear out other tasks in time for CM-DCS to enter the Commit phase. It terminates all non-CM-DCS CM agent tasks on the Destination, allowing a CM-DCS run to obtain a hard-lock and commit the changes.

- If **`CSID=`** is omitted, the default is the Destination's ID.
- Use KILLTASKS in a script after a synchronization terminates with `BATCHRC=003` (hard-lock timeout).

DMABATCH ACTION=RESET

This command will reset an incomplete synchronization session to its initial state, cause an immediate unlock of both CM Configuration Servers, and release staged resources (if any). Any subsequent synchronization of the defined synchronization pair will start from scratch.

- Use RESET in a script after a synchronization fails (BATCHRC not = 000) if it is determined that the synchronization cannot be resumed in a timely manner and the CM Configuration Servers cannot be left locked.

```
DMABATCH ACTION=SOFTLOCK [CSID=id]
DMABATCH ACTION=UNLOCK [CSID=id]
DMABATCH ACTION=HARDLOCK [CSID=id]
```

These commands are intended for use with multiple synchronizations from a shared Source database.

- Soft-locking the Source guarantees that resource data that is generated for Source Domains will be retained in cache instead of being recalculated for each synchronization, thereby increasing performance.
- If **`CSID=`** is omitted, the default is the Destination's ID.
- If the HARDLOCK command is run, the specified CM Configuration Server will be hard-locked, thereby preventing CM agents from connecting. Also, any CM agent tasks that are running on the CM Configuration Server are killed.

  The specified CM Configuration Server must currently be unlocked. The default is the Destination CM Configuration Server.

  > This operation is intended for use in environments in which multiple CM Configuration Servers share a database—a practice that HP *advises against*.

CSID Value Considerations

- If **`CSID=`** is omitted, the default is the Destination CM Configuration Server's ID.
- If **`CSID`** ≠ the Source or Destination CM Configuration Server (master or slave), the -port and -address of the CM Configuration Server must be specified.

Results of DMABATCH

The results of a DMABATCH synchronization are found in the *batch-message* variable, BATCHMSG, and the associated *batch return-code* variable, BATCHRC (see Table 12 on page 53), in the ZMGRSYNC object.

- After the Differencing step, a BATCHRC of `000` indicates that no domain differences were found.

  The associated BATCHMSG message is "`No differences found.`"

- During the Staging and Commit phases of CM-DCS, the `000` return code indicates that the phase was successful.

  The corresponding BATCHMSG is "`Successfully Completed.`"

A Troubleshooting the CM Distributed Configuration Server

At the end of this appendix, you will have had the opportunity to learn more about:

- Troubleshooting CM Distributed Configuration Server issues with the help of:
  - — Logs
  - — Tracing
  - — An EDMAMS verb

Logs to Obtain

For CM Distributed Configuration Server problems, `dmabatch.log` and the Destination CM Configuration Server log are needed. Although, it is unlikely that the Source CM Configuration Server log will be helpful, do not discard it or allow it to be overwritten before contacting HP Technical Support.

Log Error Messages

The five log messages that are shown below correspond to the domain eligibility rules. Depending on the circumstances of the failed synchronization, these messages might be found in `dmabatch.log`.

- The "last synchronization" date refers to the local time on the Destination CM Configuration Server.

Table 13 Domain eligibility error messages

Message
`Skipping Domain [`*`domain`*`] because owners at source <`*`src ID`*`> and destination <`*`dest ID`*`> do not match`
`Skipping Domain [`*`domain`*`] because cannot synchronize to owner`
`Skipping Domain [`*`domain`*`] because owners at source <`*`src ID`*`> and destination <`*`dest ID`*`> do not match`
`Skipping Domain [`*`domain`*`] because non-authoritative replica: updated (<`*`date`*`> <`*`time`*`>) since last synchronization (<`*`date`*`> <`*`time`*`>)`
`Skipping Domain [`*`domain`*`] because possible DB regression - destination replica (<`*`date`*`> <`*`time`*`) more recent than source (<`*`date`*`> <`*`time`*`>)`

Log and Object Locations

The default locations for the CM-DCS objects and logs are `IDMLIB` and `IDMLOG`, respectively.

➤ The values of these variables can be overridden by the `-libpath` and `-logpath` options in the file, `dmabatch.rc`.

Activating Tracing for CM-DCS

In the MGR_TRACE section of the `edmprof` file, add the following setting and value:

```
DMA=YES
```

The DMA acronym represents *Distributed Manager Adapter*, the original name of the CM Distributed Configuration Server.

CM Distributed Configuration Server Objects and Files

CM Distributed Configuration Server Objects

Obtain the following objects from the default CM Distributed Configuration Server directory. If CM-DCS is running on a desktop with either a CM agent or CM Administrator, look in `IDMLIB`.

- ZMANAGER contains the properties of all the CM Configuration Servers that have been defined to CM-DCS. TP parameters (including TP trace level) are defined here, per CM Configuration Server.
- ZMGRSYNC contains information about the synchronization pair, including any applicable password information. This object is refreshed when: 1) another synchronization pair is defined and 2) when there is a domain change. The object retains information of saved CM-DCS sessions for subsequent recall.

  The non-TP trace level is determined by ZMGRSYNC.ZTRACEL.

  There are two ZMGRSYNC variables that relate to DMABATCH—BATCHMSG and BATCHRC. These are described in Table 12 on page 53.

Settings in the `dmabatch.rc` file will always supersede settings in the ZMANAGER and ZMGRSYNC objects.

CM Distributed Configuration Server Files

This section defines the CM-DCS `.MK`, `.DAT`, and `.IDX` files. Each of these files is preceded by a domain name, as in:

```
domain.dat
```

.MK

These are *metakit* database files that contain, in a compact and searchable format, a domain's metadata—its instances and class definitions.

- `.MK` files are built on all platforms, on the Source and Destination CM Configuration Servers.

.DAT

These files cache a domain's *small resource* files. This is a performance feature that minimizes CM Configuration Server Database file operations.

- `.DAT` files are built on Solaris and Windows platforms only; on Source CM Configuration Servers only.

The amounts of free disk space and the space used by metakits and resource caches, before and after each domain analysis operation, are shown in `dmabatch.log`.

.IDX

These are *index* files for the corresponding .DAT files.

- `.IDX` files are built on Solaris and Windows platforms only; on Source CM Configuration Servers only.

The EDMAMS Utilities

EDM Access Method Services (**EDMAMS**) is a set of utilities that can be used to create, delete, copy, change, and list CM Configuration Server Database objects.

For more information on the EDMAMS verbs, refer to the *HP OpenView Configuration Management Configuration Server User Guide* (*CM Configuration Server Guide*).

One of the EDMAMS verbs, UPDATE_MGRIDS, can be used to update the MGR_ID, CM Configuration Server name, owning MGR_ID, and owning CM Configuration Server name.

UPDATE_MGRIDS

- If **DOMAIN** is omitted, all domains are updated.
- All keywords are optional; however, at least one keyword other than **DOMAIN** must be specified.

```
ZEDMAMS VERB=UPDATE_MGRIDS(,FILE=file name)(,DOMAIN=domain
name)(,CLASS=class name)(,MNAME=local CM-CS name)
(,MID=local CM-CS ID)(,MMNAME=owning CM-CS name)
(,MMID=owning CM-CS ID)
```

Domain Eligibility

- *What if no domains are eligible for synchronization?*

  If no domains are presented as eligible for synchronization, make sure that both CM Configuration Servers were installed as CM-DCS-enabled CM Configuration Servers. It might be necessary to use the UPDATE_MGRIDS verb to rectify this issue.

  ➤ Refer to the *CM Configuration Server Guide* for more information about the MANAGER_TYPE setting of the MGR_STARTUP section of the `edmprof` file.

B Product Name Changes

If you have used Radia in the past, and are not yet familiar with the newly rebranded HP terms and product names, Table 14 below will help you identify naming changes that have been applied to the Radia brand.

Table 14 Product Name and Term Changes

New Name/Term	Old Name/Term
CM agents	Radia clients
HP OpenView Configuration Administrator	Radia Administrator Workstation
HP OpenView Configuration Management	Radia
HP OpenView Configuration Management Configuration Server	Radia Configuration Server, RCS
HP OpenView Configuration Management Distributed Configuration Server	Radia Distributed Configuration Server, Radia DCS, DMA
HP OpenView Configuration Management Configuration Server Database	Radia Configuration Server Database, Radia Database
HP OpenView Configuration Management Policy Server	Radia Policy Manager, Radia Policy Server, RPS
HP OpenView Configuration Management Proxy Server	Radia Proxy Server

Index

.

.dat files, 62

.idx files, 62

.mk files, 62

A

access levels, 6

ADMIN_LIST, 43, 45

B

BATCHMSG, 53

BATCHRC, 53, 56

BATCHRC and BATCHMSG values, 53

C

CM Admin CSDB Editor, 23

CM Admin Packager, 23

CM Admin Publisher, 23

CM Configuration Server
- synchronization eligibility, 19

CM Distributed Configuration Server
- communications protocol, 28
- configuration file, 48
- defined, 13
- description, 16
- Destination CM Configuration Server, 17
- Destination component installation, 33
- directories, 29
- domain eligibility rules, 23
  - log error messages, 60
- installation
  - Destination component, 33
  - Source component, 32
- installation options, 28
  - Destination component, 28
  - Source component, 28
- logs, 24, 60
  - CM Configuration Server logs, 60
  - DMABATCH.LOG, 60
  - log error messages, 60
- objects, 24
  - saved, 61
  - ZMANAGER, 61
  - ZMGRSYNC, 61
- processor requirements, 28
- recommendations and requirements, 28
- saved objects, 61
- security, 44
  - CM Configuration Server

security

  - settings, 44
  - password, 44
  - setting up, 44
  - user ID, 44
- Source CM Configuration Server, 17
- Source component installation, 32
- space requirements, 30
- terminology, 12
  - CM Distributed Configuration Server, 13
  - container file, 14
  - Destination CM Configuration Server, 13
  - domain ownership, 13
  - foreign-owned domain, 14
  - middle-tier CM Configuration Server, 14
  - peer synchronization, 13
  - self-owned domain, 13
  - Source CM Configuration Server, 13
  - synchronization, 13
  - synchronization pair, 13
  - unrelated domains, 14

CM Distributed Configuration Server-specific terminology, 12

CM Integration Server, 18, 39
- defined, 13

CM Portal, 18

CM Proxy Server, 18

CM-DCS
- configuration file, 48

configuring CM Distributed Configuration Server, 24

container file, 14

copyright notices, 2

current MGR_ID, 20

customer support, 6

D

Destination CM Configuration Server, 19
- defined, 13
- installation, 33
- MANAGER_TYPE setting, 20
  - DISTRIBUTED, 19
  - SERVER, 19
- performance improvements, 20

Destination component, 18
- installation, 33
- temporary directory, 39

directories
- CM Distributed Configuration Server, 29

DMA_TIMEOUT, 44

DMABATCH
- hardlock, 57
- kill tasks, 56
- quiesce, 56
- reset, 57
- resume, 56
- softlock, 57
- unlock, 57

dmabatch.exe, 24

DMABATCH.LOG, 60

dmabatch.rc options, 48

DMASTATS, 51, 52
- BATCHRC, 53
- fields defined, 52
- REPORTID, 53

document map, 12

documentation updates, 4

domain eligibility, 23
- error messages, 60
- rules, 23
  - domain deletion, 23

domain naming considerations, 21

domain ownership, 20
- defined, 13
- establishing, 20

domains
- current MGR_ID, 20
- domain name, 20
- eligibility, 23
  - rules, 23
- foreign-owned, 20
- local updates, 23
- owning MGR_ID, 20
- self-owned, 20
- unrelated, 23

E

EDMAMS, 62
- UPDATE_MGRIDS, 63

edmprof file, 42, 45
- MGR_DMA, 43
- MGR_STARTUP, 19, 20, 42
- MGR_TRACE, 61

EDMSIGNR, 45

eligibility, domains, 23

F

files
- .dat, 62
- .idx, 62
- .mk, 62

foreign-owned domain, 20
- defined, 14

H

hardlock Source CM Configuration Server Database, 57

I

IDMLIB, 60

IDMLOG, 60

installation
- Destination component of CM Distributed Configuration Server, 33
- Source component of CM Distributed Configuration Server, 32

K

kill (non CM-DCS agent) tasks, 56

L

legal notices
- copyright, 2
- restricted rights, 2
- warranty, 2

local updates, 23

M

MANAGER_TYPE setting, 19
- performance improvements, 20
- using to improve performance, 20

MGR_DMA, 42, 43, 45
- ADMIN_LIST, 43
- DMA_TIMEOUT, 44
- SECURITY_METHOD, 43, 45

MGR_ID, 20, 43

MGR_STARTUP, 42
- MANAGER_TYPE, 19, 42
  - DISTRIBUTED vs. SERVER, 19, 20
- MGR_ID, 42
- MGR_NAME, 42
- TCP_PORT, 43

MGR_TRACE, 61

middle-tier CM Configuration Server, 16, 20
- defined, 14
- MANAGER_TYPE setting, 20
  - SERVER, 20
- performance improvements, 20

O

owning MGR_ID, 20

P

peer synchronization, 16
- defined, 13

pre-installation notes, UNIX, 30

processor requirements
- CM Distributed Configuration Server, 28

PUTPROF, 51

Q

quiesce
- qtype, 56
  - task, 56
  - trans, 56

quiesce Destination CM Configuration Server Database, 56

R

REPORTID, 53
- values defined, 53

reset synchronization session, 57

restricted rights legend, 2

resume synchronization session, 56

S

saved CM Distributed Configuration Server objects, 61

security on the CM Configuration Server, 45

security, setting up in CM Distributed Configuration Server, 44

SECURITY_METHOD, 43, 45

self-owned domain, 20
- defined, 13

setting up security in CM Distributed Configuration Server, 44

simultaneous synchronizations, 24

softlock Source CM Configuration Server Database, 57

Source CM Configuration Server, 19
- defined, 13
- installation, 32
- MANAGER_TYPE setting, 19
  - DISTRIBUTED, 19
  - SERVER, 19

source component, 18

Source component
- installation, 32
- temporary directory, 39

support, 6

supported platforms, 29

synchronization
- defined, 13

synchronization pair, 19
- control information, 17
- defined, 13
- ZMGRSYNC, 61

synchronization, domain eligibility, 23

synchronizations
- simultaneous, 24

T

technical support, 6

-temp-dir, 39

temporary directories, 39
- Destination, 39
- Source, 39
- -temp-dir, 39
- TMPDIR, 39

terminology, 12
- CM Distributed Configuration Server, 12

TMPDIR, 39

troubleshooting CM Distributed Configuration Server
- CM Configuration Server property information, 61
- CM Distributed Configuration Server logs, 60
- domain eligibility, 63
- EDMAMS utility, 63
  - UPDATE_MGRIDS, 63
- files
  - .dat, 62
  - .idx, 62
  - .mk, 62
- IDMLIB, 60, 61
- IDMLOG, 60
- INI files, 60
- no eligible domains, 63
- synchronization pair information, 61
- tracing, 61

U

UNIX pre-installation notes, 30

unlock Source CM Configuration Server Database, 57

unrelated domains, 23
- defined, 14

updates to doc, 4

W

warranty, 2

Z

ZMANAGER, 61
- CM Configuration Server property information, 61

ZMGRSYNC, 61
- BATCHMSG, 57
- BATCHRC, 57
- CM Distributed Configuration Server sessions saved, 61
- synchronization pair saved, 61

ZUSERID, 52, 53