

# HP Client Automation Enterprise Distributed Configuration Server

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

Software Version: 7.80

---

## Installation and Configuration Guide

Manufacturing Part Number: None

Document Release Date: November 2009

Software Release Date: November 2009



## 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

© Copyright 1993–2009 Hewlett-Packard Development Company, L.P.

### 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  
Copyright Mihai Bazon, 2002, 2003

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
  - The number before the period identifies the major release number.
  - The first number after the period identifies the minor release number.
  - The second number after the period represents the minor-minor release number.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

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

**<http://h20230.www2.hp.com/selfsolve/manuals>**

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

**<http://h20229.www2.hp.com/passport-registration.html>**

Or click the **New users - please register** link on the HP Passport login page.

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

**Table 1** below lists the changes that were made to this document.

**Table 1 Documentation changes**

| Chapter    | Version | Changes   |
|------------|---------|---|
| Title Page | 7.80    | Updated product version number and release date for 7.80.   |
| All        | 5.00    | Revised all directory paths. The default directory paths for CM products have been revised to: <ul style="list-style-type: none"><li>• Program Files\Hewlett-Packard\CM (Windows)</li></ul> And... <ul style="list-style-type: none"><li>• HP/CM (UNIX)</li></ul> |
| 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   | Version | Changes  |
|-----------|---------|--|
| Chapter 2 | 7.20    | Page 19, inserted a note regarding a limitation with SSL functionality.  |
| Chapter 2 | 7.50    | Page 19, inserted a new section, <a href="#">IP Networking Support</a> .   |
| Chapter 3 | 5.00    | Updated this chapter to include the new installation steps that were introduced in this version of CM-DCS.   |
| Chapter 3 | 5.10    | <p>Page 34, there is a new window (CM Distributed Configuration Server (Source) Install CM Integration Server) in the Source component installation. In this window, a CM administrator can specify into which directory the CM Integration Server and user-interface web services files will be installed, and whether it will be <b>shared</b> by other CM components or <b>dedicated</b> to the CM-DCS.</p> <p>Note: If the CM Integration Server will be dedicated to the CM-DCS, two additional port-specification windows will be presented during the installation.</p> |
| Chapter 4 | 5.00    | Removed most of the information from <i>Chapter 5, Setting up a Distributed Configuration Server Synchronization</i> , because it pertained to GUI-configuration procedures. The information that is still relevant was combined with <i>Chapter 4, Distributed Configuration Server Security</i> . The result is a revised Chapter 4, <a href="#">The EDMPROF File and DCS Security</a> .   |
| Chapter 5 | 5.00    | Removed most of the information from <i>Chapter 6, Configuring Distributed Configuration Server Options</i> , because it pertained to GUI-configuration procedures. The information that is still relevant was combined with <i>Chapter 7, Distributed Configuration Server's DMABATCH</i> . The result is a revised Chapter 5, <a href="#">Distributed Configuration Server Options and DMABATCH</a> .  |
| Chapter 5 | 5.10    | Page 53, added the dmabatch option <b>-dataless</b> to <a href="#">Table 7</a> .   |
| Chapter 5 | 7.20    | <p>Page 53, added two new options <b>-download</b> and <b>-max-deletes</b> to <a href="#">Table 7</a>.</p> <p>Additional information is in the sections, <a href="#">Download</a> and <a href="#">Maximum Deletions</a>, starting on page 56.</p>  |
| Chapter 5 | 5.10    | Page 56, added the dmabatch option <b>-dataless</b> to <a href="#">Table 8</a> .   |
| Chapter 5 | 7.80    | Page 52, updated information about Source and Destination configuration files: <code>dcs.cfg</code> and <code>dmabatch.rc</code> .   |

| <b>Chapter</b> | <b>Version</b> | <b>Changes</b>   |
|----------------|----------------|--|
| 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/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport)**

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 an active support contract. To find more information about support access levels, go to the following URL:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

To register for an HP Passport ID, go to the following URL:

**<http://h20229.www2.hp.com/passport-registration.html>**





# Contents

|   |           |
|---|-----------|
| <b>1 Introduction .....</b>   | <b>13</b> |
| Using this Guide with Core and Satellite Servers .....              | 14        |
| Documentation Map .....   | 14        |
| Terminology .....   | 14        |
| <b>2 Introduction to the Distributed Configuration Server .....</b> | <b>17</b> |
| Overview .....  | 18        |
| Distributed Configuration Server .....                              | 18        |
| IP Networking Support .....   | 19        |
| Distributed Configuration Server Components .....                   | 19        |
| Source vs. Destination .....  | 20        |
| Two Configuration Servers: A Synchronization Pair .....             | 21        |
| Configuration Server Eligibility .....                              | 21        |
| Improving Performance using <code>MANAGER_TYPE</code> .....         | 22        |
| Domain Ownership .....  | 22        |
| Domain Naming Considerations .....                                  | 23        |
| One Owner vs. Multiple Owners .....                                 | 23        |
| One Owning Configuration Server .....                               | 23        |
| Multiple Owning Configuration Servers .....                         | 24        |
| Domain Eligibility .....  | 25        |
| Selecting Domains .....   | 25        |
| Domain Eligibility Rules .....                                      | 25        |
| Configuring Distributed Configuration Server .....                  | 26        |
| Distributed Configuration Server: Batch Mode .....                  | 26        |
| Synchronization Logs .....  | 26        |
| Simultaneous Synchronizations .....                                 | 27        |
| Distributed Configuration Server Planning .....                     | 27        |
| When to Use Distributed Configuration Server .....                  | 27        |

|          |   |           |
|----------|---|-----------|
| <b>3</b> | <b>Installing the Distributed Configuration Server .....</b>      | <b>29</b> |
|          | Two-Phase Installation .....                                      | 30        |
|          | System Requirements.....  | 30        |
|          | Platform Support .....  | 30        |
|          | Distributed Configuration Server Directories.....                 | 31        |
|          | Source .....  | 31        |
|          | Destination.....  | 31        |
|          | Distributed Configuration Server Space Requirements.....          | 32        |
|          | Installing the Distributed Configuration Server .....             | 32        |
|          | UNIX Pre-Installation Notes .....                                 | 32        |
|          | Installing the DCS Source Component.....                          | 33        |
|          | Installing the DCS Destination Component.....                     | 37        |
|          | Post-installation Notes .....                                     | 42        |
|          | Setting a Temporary Directory .....                               | 42        |
|          | Source Component .....  | 43        |
|          | Destination Component.....  | 43        |
| <b>4</b> | <b>The EDMPROF File and DCS Security .....</b>                    | <b>45</b> |
|          | The EDMPROF File .....  | 46        |
|          | Editing the EDMPROF File .....                                    | 46        |
|          | MGR_STARTUP Section.....  | 46        |
|          | MGR_DMA Section.....  | 48        |
|          | Setting up Security.....  | 48        |
|          | Native Operating-System Security .....                            | 48        |
|          | Configuration Server Security Settings .....                      | 49        |
| <b>5</b> | <b>Distributed Configuration Server Options and DMABATCH.....</b> | <b>51</b> |
|          | Distributed Configuration Server Configuration Files .....        | 52        |
|          | dcs.cfg.....  | 52        |
|          | dmabatch.rc .....   | 52        |
|          | Download.....   | 55        |
|          | Maximum Deletions .....   | 56        |
|          | Configuration Object Equivalents.....                             | 56        |
|          | DMASTATS.....   | 57        |

|   |           |
|---|-----------|
| ZUSERID .....   | 59        |
| DMABATCH Command-line Options .....                                 | 60        |
| Reset .....   | 60        |
| Deferred Commit .....   | 60        |
| DMABATCH Scripting Commands .....                                   | 61        |
| DMABATCH Line Commands .....  | 61        |
| CSID Value Considerations .....                                     | 63        |
| Results of DMABATCH .....   | 63        |
| <b>A Troubleshooting the Distributed Configuration Server .....</b> | <b>65</b> |
| Logs to Obtain .....  | 66        |
| Log Error Messages .....  | 66        |
| Log and Object Locations .....                                      | 66        |
| Activating Tracing for DCS .....                                    | 67        |
| Distributed Configuration Server Objects and Files .....            | 67        |
| Distributed Configuration Server Objects .....                      | 67        |
| Distributed Configuration Server Files .....                        | 67        |
| The EDMAMS Utilities .....  | 68        |
| UPDATE_MGRIDS .....   | 69        |
| Domain Eligibility .....  | 69        |
| <b>Index .....</b>  | <b>71</b> |



---

# 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 Client Automation Distributed Configuration Server (Distributed Configuration Server)**.
- Become familiar with some of the terminology that is specific to Distributed Configuration Server (**DCS**).

# Using this Guide with Core and Satellite Servers



If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started and Concepts Guide* as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

## Documentation Map

This section provides an overview of this book; this will aid in locating specific information about the Distributed Configuration Server.

Chapter 2, [Introduction to the Distributed Configuration Server](#) describes Distributed Configuration Server, including: how it works; the roles of the two DCS components; Configuration Server eligibility, domain ownership, and domain eligibility.

Chapter 3, [Installing the Distributed Configuration Server](#) details the installation of the two DCS components, including system recommendations.

Chapter 4, [The EDMPROF File and DCS Security](#) discusses the `edmpprof` file sections that are relevant to DCS; and setting up security for DCS.

Chapter 5, [Distributed Configuration Server Options and DMABATCH](#) provides a look at the DCS configuration file and its options; and the DMABATCH command-line options.

Appendix A, [Troubleshooting the Distributed Configuration Server](#) discusses troubleshooting DCS, including logs, tracing, and domain eligibility.

## Terminology

[Table 2](#) on page 15 describes the 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 2 Distributed Configuration Server Terminology**

| <b>Term</b>  | <b>Description</b>  |
|--|---|
| Distributed Configuration Server                   | The Distributed Configuration Server is an extension of the Configuration Server. It synchronizes Configuration Server Databases (CSDB) that are running on separate (DCS-enabled) machines across an enterprise. |
| Integration Server                                 | The HTTP file server of Client Automation. It gets installed on a Source Configuration Server in order to facilitate multiple concurrent file transfer sessions and the creation of the container file.           |
| Source Configuration Server<br><b>(master)</b>     | In a DCS synchronization, the Configuration Server from which the Destination Configuration Server will receive database changes.   |
| Destination Configuration Server<br><b>(slave)</b> | In a DCS synchronization, the (target) Configuration Server on which CSDB changes will be replicated.<br>Note: This is <i>always</i> a replica of the Source database.  |
| Synchronization                                    | The replicating of administrator-specified domains from one Configuration Server Database (Source Configuration Server) to another (Destination Configuration Server).  |
| Peer Synchronization                               | Synchronizing a Domain on a Destination Configuration Server from a Source Configuration Server that does not own the Domain.<br>See <a href="#">Foreign-Owned Domain</a> in this table.                          |
| Synchronization Pair                               | The two Configuration Servers that have been selected as the Source and Destination.  |
| Domain Ownership                                   | All Domains are “owned” by a Configuration Server. Domains are either <b>self-owned</b> or <b>foreign-owned</b> .<br>See <a href="#">Domain Ownership</a> on page 22.   |
| Self-Owned Domain                                  | A Domain that is owned by the current Configuration Server.<br>Note: In order for a Domain to be self-owned, the owning MGR_ID and current MGR_ID must be identical.  |
| Foreign-Owned Domain                               | A Domain that is owned by a Configuration Server other than the current one.<br>Note: If the owning MGR_ID and current MGR_ID are different, the Domain is foreign-owned.   |

| <b>Term</b>                      | <b>Description</b>  |
|----------------------------------|---|
| Unrelated Domains                | Domains that are not owned by the same Configuration Server—that is, they do not have the same owning MGR_ID.   |
| Middle-tier Configuration Server | A middle-tier Configuration Server is not an HP product. Rather this term is used exclusively to reference any Configuration Server on which the Source and Destination components are installed so that it can support peer synchronizations.  |
| Container File                   | <p>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.</p> <p>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 Configuration Server Database is hard-locked.</p> |
| edmprof file                     | <p>This is the text file in which the operational parameters of the Configuration Server are specified.</p> <ul style="list-style-type: none"> <li>• On UNIX platforms, this file is <code>.edmprof</code></li> <li>• On Windows platforms, this file is <code>edmprof.dat</code>.</li> </ul> <p>Note: This guide uses this non-platform specific, generic reference.</p>   |



---

## 2 Introduction to the Distributed Configuration Server

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

- How the HP Client Automation Distributed Configuration Server (Distributed Configuration Server, DCS) works to synchronize HP Client Automation Configuration Server Databases.
- Why there are two Distributed Configuration Server components, and the role of each in ensuring a successful synchronization.
- How to define a pair of HP Client Automation Configuration Servers (Configuration Servers) for synchronization based on Configuration Server *eligibility* and *domain ownership*.
- The role of Configuration Server Database (CSDB) domains in DCS 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 DCS process*, which will aid in troubleshooting.

# Overview

Distributed Configuration Server is a tool that enables an administrator to manage multiple **Configuration Server Databases (CSDBs)** in a networked environment.

An administrator can use DCS to replicate domains from one CSDB to another. This means that enterprise-wide changes can be made once, on one Configuration Server machine, then simply distributed to (replicated on) multiple down-line 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.

## Distributed Configuration Server

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

► Additional DCS *dependency*, *directory*, and *requirement* information is presented in the section [Distributed Configuration Server Directories](#) starting on page 31.

For more information on the functionality of the DCS components, see the section, [Distributed Configuration Server Components](#) starting on page 19.

In a **multi-tier** configuration, both components can be installed on the same machine in order to accommodate *peer synchronizations* via a *middle-tier Configuration Server*. (Peer synchronizations and middle-tier Configuration Servers are defined in [Table 2](#) on page 15.)

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

synchronization pair (see [Two Configuration Servers: A Synchronization Pair](#) on page 21).

In a synchronization, DCS compares the control information of one CSDB with that of another, for the domains that have been selected.

- ▶ If SSL functionality is used during a DCS synchronization, files larger than 2 GB will fail.

## IP Networking Support

With this release, HP Client Automation adds support for **IPv6**—the latest version of the internet protocol addressing structure—to its Windows-based Core and Satellite servers. The Core and Satellite servers can now use either IP version 4 (**IPv4**) or IP version 6 (**IPv6**) for server-to-server communications. HPCA agent communications, however, are currently limited to IPv4. For details, refer to the appendix, *IPv6 Networking Support*, in the *HPCA Enterprise User Guide*.

- ▶ HP Client Automation environments that use the traditional, component-based, HPCA server installations will continue to be supported on IPv4 only.

## Distributed Configuration Server Components

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

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

With the DCS components installed on the Configuration Server machines, 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 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 Configuration Server that is going to function as the master in a synchronization. This component contains the Integration Server, the product suite's HTTP server.



#### Integration Server Notes

- For a brief description of Integration Server and how it relates to DCS, see [Integration Server](#) below.
- For a detailed description of Integration Server, refer to the *HP Client Automation Essentials Guide (Essentials Guide)*, available in the Client Automation 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 CSDB instance.

### Integration Server

Integration Server is the Client Automation 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 2](#) starting on page 15).

Integration Server is not a separately licensed HP product. It integrates several independent modules—**HP Client Automation Portal (Portal)** and

**HP Client Automation Proxy Server (Proxy Server)**—giving them access to all the functions and resources under its control.

### Destination Component

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

## Two Configuration Servers: A Synchronization Pair

Two Configuration Servers, one defined as the Source and the other as the Destination, comprise a 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.

DCS will accept one synchronization pair only, per execution. Operationally, because a synchronization can go in only one direction, this means that if two Configuration Servers (for example, MGR\_001 and MGR\_002) need domains from one another, two DCS executions must be done—with MGR\_001 being the Source in one synchronization, and MGR\_002 being the Source in the other.

## Configuration Server Eligibility

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

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

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

or

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



All 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](#) below, for performance-improvement information.

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

## Improving Performance using MANAGER\_TYPE

Typically, Destination and middle-tier Configuration Servers (see [Middle-tier Configuration Server](#) in [Table 2](#) on page 16) get database updates from their up-line Source Configuration Server only. Therefore, some default database administrative processes are not necessary. HP indicates that disabling these unnecessary processes will improve performance.

- If a DCS-enabled Configuration Server is going to be a Destination or middle-tier Configuration Server—getting its updates from a Source Configuration Server only and not managed via any other process—you can improve its performance by setting:

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

## Domain Ownership

Configuration Server Database domains on each 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 CSDB is installed.
- When a domain is added to a CSDB.



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

A self-owned domain is a CSDB domain that is owned by the current Configuration Server. The owning MGR\_ID and current MGR\_ID are the same.

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

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 Configuration Server cannot contain two domains with the same name.
- A Configuration Server cannot obtain one of its self-owned domains from a Configuration Server that foreign-owns the domain. For example, MGR\_001 cannot receive from another 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 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 Configuration Server, thereby centralizing control; or to disperse control by establishing domain ownership at several 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 [Distributed Configuration Server Planning](#), starting on page 27.

## One Owning Configuration Server

[Table 3](#) on page 24 lists the benefits and drawbacks of one Configuration Server owning all the domains.

**Table 3 One domain-owning Configuration Server**

| <b>Advantages</b>                                    | <b>Disadvantages</b>  |
|--|---|
| Control of all applications, access rules, and users | Central control might make the database very large, depending on the organization and structure |
| One Configuration Server Database to backup          | Does not align well with highly decentralized organizations                                     |
| Data flow throughout the environment is one-way      | Data flow throughout DCS is one-way   |
| Aligns with highly centralized organizations         |   |

## Multiple Owning Configuration Servers

Table 4 below lists the benefits and drawbacks of domain ownership being assigned to multiple Configuration Servers.

**Table 4 Multiple domain-owning Configuration Servers**

| <b>Advantages</b>  | <b>Disadvantages</b>  |
|--|---|
| Aligns readily with highly decentralized organizations   | Does not align well with highly centralized organizations         |
| Databases are smaller and indicative of regional Source Configuration Servers                        | Multiple 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 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 Configuration Servers                         |   |





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

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

## Domain Eligibility

The list of domains that are eligible for synchronization is dynamically compiled by 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 administrative components (such as **HP Client Automation Administrator Configuration Server Database Editor (Admin CSDB Editor)**, **HP Client Automation Administrator Packager (Packager)**, and **HP Client Automation Administrator Publisher (Publisher)**).

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

## Selecting Domains

It is not necessary to synchronize all eligible domains between two DCS-enabled 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 DCS domain synchronization eligibility rules are listed below. These apply to each domain independently. See [Log Error Messages](#) on page 66.

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



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

- Domains that are not owned by the same 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 Client Automation component, it cannot be used as the Source in a *peer synchronization*.
  - ▶ A local update occurs when a CSDB is updated by a Client Automation component (such as Admin CSDB Editor, Admin Publisher, and Admin Packager) other than Distributed Configuration Server.
- When it is possible to make such a distinction, the 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.

## Configuring Distributed Configuration Server

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

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

### Distributed Configuration Server: Batch Mode

The command-line mode (also known as the **batch** mode) of 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 [Distributed Configuration Server Options and DMABATCH](#), on page 51.

### 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 DCS synchronization.

## Simultaneous Synchronizations

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

## Distributed Configuration Server Planning

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

### When to Use Distributed Configuration Server

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

- To replicate CSDB 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 DCS infrastructure requires knowledge of:

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



---

# 3 Installing the Distributed Configuration Server

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

- Install the Distributed Configuration Server **Source** component.
- Install the Distributed Configuration Server **Destination** component.



If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started and Concepts Guide* as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

## Two-Phase Installation

In order set up a distributed Configuration Server synchronization environment, DCS enables a Client Automation administrator to install:

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

The installations are outlined in [Installing the Distributed Configuration Server](#), starting on page 32.

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



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

For a detailed description of these components, see [Source Component](#) and [Destination Component](#) on page 20.

## System Requirements

To ensure the successful installation and operation of DCS, the following system requirements are recommended.

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

### Platform Support

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

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

## Distributed Configuration Server Directories

This section details (by platform) the directories that are created by default by the installations of the DCS components.

### Source

If this is the initial installation of the DCS Source component (meaning there is *not* an existing 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 Integration Server element, no directories are added by the installation; however, the first execution of the DCS execution will add *IntegrationServer\_directory\data\dcs*.

### Destination

If this is the initial installation of the DCS 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 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
```

## Distributed Configuration Server Space Requirements

The amount of free disk space that is required by the DCS components will vary because it is dependent on the number of domains that are selected, their size, domain selections, and the size of the synchronization differences.

# Installing the Distributed Configuration Server

This section details the installation of the DCS. 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**.

Also, the setup files, which are in the following directories, should have execute permissions.

- `extended_infrastructure/distributed_configuration_server`



- `extended_infrastructure/distributed_configuration_server/`  
Dest
- `extended_infrastructure/distributed_configuration_server/`  
Source

Navigate to these directories and change the execute permission by using command **chmod +x setup**.

### To install the 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 HPCA Distributed Configuration Server Install Welcome window opens.
- 3 Click **Next**. The HPCA Distributed Configuration Server Install HP Software Licensing Agreement window opens.
- 4 Click **Accept**.



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

The HPCA Distributed Configuration Server Installation Component Selection window opens.

- Select either, or both, of the Distributed Configuration Server components.
- 5 Click **Next**. The HPCA Distributed Configuration Server Installation Summary window opens. It displays the 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 HPCA Distributed Configuration Server (Source) Install Welcome window will appear.

## Installing the DCS Source Component

This section describes the installation of the Source component of DCS.

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

- 1 Click **Next**. The HPCA Distributed Configuration Server (Source) Install HPCA Integration Server window opens.

In this window, specify the directory into which the Integration Server and user-interface web services files will be installed, and whether it will be shared by other Client Automation components.

- Accept the default, **Dedicated Integration Server** if the Integration Server will be dedicated to the DCS (`httpd-distributedcs`); or
- Select **Shared Integration Server** in order to have the Integration Server shared by other Client Automation components (`httpd-integrationserver`), or if you plan to continue using an existing Integration Server.

If there is an existing Integration Server, its associated (existing) configuration file (`.rc`) will be left “untouched.”



The port-specification windows that are mentioned in steps 5 (on page 36) and 6 (on page 36) will be presented only if:

- **Dedicated Integration Server** was selected in the HPCA Distributed Configuration Server (Source) Install HPCA Integration Server window

And,

- This is the first installation of a dedicated Integration Server into the installation path that was selected (i.e., the file `InstallPath/DistributedCS/httpd-distributedcs.rc` does not already exist).

Otherwise, the existing configuration file in the installation path, if any, will be used. If no existing configuration file is found, a default file—specifying default TCP/IP and SSL ports **3466** and **443**, respectively—will be created.

Furthermore, the presence/absence of these port-specification windows does not affect the remainder of the installation.



### UNIX Note

The new Integration Server standard configuration file names (`httpd-integrationserver` for shared; `httpd-distributedcs` for dedicated), will have to be specified at Integration Server startup via a `-config` parameter. For example:

- `nvdkit httpd.tkd -config httpd-integrationserver.rc`

Or

- `nvdkit httpd.tkd -config httpd-distributedcs.rc`

- 2 Click **Next**. The HPCA Distributed Configuration Server (Source) Install HP Software License Agreement window opens.
- 3 Click **Accept**.



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

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



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

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

- If the installation program detects an existing Client Automation element (such as an HPCA agent, HPCA Administrator, or a previous version of DCS), 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 Client Automation 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.

- 4 Click **Next**. The HPCA Distributed Configuration Server (Source) Install Database Path window opens.

The Source HPCA-CS Database Path field displays the directory in which the 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.

- 5 Click **Next**. The HPCA Distributed Configuration Server (Source) Install HPCA Integration Server TCP/IP Port window opens.



This window will be presented only if:

- **Dedicated Integration Server** was selected in the HPCA Distributed Configuration Server (Source) Install HPCA Integration Server window

And

- This is the first installation of the Integration Server into the installation path that was selected.

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

- Accept the default Integration Server TCP/IP port that is displayed, **3473** (*recommended*); or
- Specify a valid 3- to 5-digit Integration Server TCP/IP port.

- 6 Click **Next**.



Due to internal processing, this window might appear to be “frozen” for up to a minute. Please wait while the processing completes.

The HPCA Distributed Configuration Server (Source) Install HPCA Integration Server SSL Port window opens.

- ▶ This window will be presented only if:
  - **Dedicated Integration Server** was selected in the HPCA Distributed Configuration Server (Source) Install HPCA Integration Server window

And

- This is the first installation of the Integration Server into the installation path that was selected.

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

- Accept the default Integration Server SSL port that is displayed, **444** (*recommended*); or
- Specify a valid 3- to 5-digit Integration Server SSL port.

7 Click **Next**.

- ▶ Due to internal processing, this window might appear to be “frozen” for up to a minute. Please wait while the processing completes.

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

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

8 To accept the specified settings, click **Install**. The HPCA Distributed Configuration Server (Source) Install Finish window opens.

9 Click **Finish**. The Source component of HPCA Distributed Configuration Server has successfully installed.

- ▶ If the installation of the DCS Destination component was also selected, it will automatically start now.

## Installing the DCS Destination Component

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

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

1 Click **Next**. The HPCA 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 HPCA Distributed Configuration Server (Destination) Install Installation Location window opens.



In the HPCA 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 DCS Destination component's files will be installed.

- If the installation program detects any existing Client Automation element (such as an HPCA agent, HPCA Administrator, or a previous version of DCS), 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 Client Automation 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 Configuration Server is installed on this machine, the information for the next three windows (Local Configuration Server ID and Local Configuration Server Ports [TCP/IP and SSL]) will be read from the `edmprof` file of the Configuration Server, and these windows will not appear during this installation.

Continue with step 4 on page 39.

If a 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 that is requested.

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

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

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

- 4 Click **Next**. The HPCA Distributed Configuration Server (Destination) Install Source HPCA Configuration Server Host Address window opens.



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

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

- Specify the IP address of the Source 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 HPCA Distributed Configuration Server (Destination) Install Source HPCA Configuration Server ID window opens.

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

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

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



The installation will accept any valid 3-character, hexadecimal 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

Configuration Server that was designated in the previous step; the installation will not perform any type of Configuration Server ID verification in the environment.

- 6 Click **Next**. The HPCA Distributed Configuration Server (Destination) Install Source HPCA Configuration Server TCP/IP Port window opens.

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



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

- Accept the default Configuration Server TCP/IP port that is displayed, **3464** (*recommended*); or
- Specify a valid 3- to 5-character decimal Configuration Server TCP/IP port.

- 7 Click **Next**. The HPCA Distributed Configuration Server (Destination) Install Source HPCA Configuration Server SSL Port window opens.

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

- Accept the default Configuration Server SSL port that is displayed, **443** (*recommended*); or
- Specify a valid 3- to 5-character decimal Configuration Server SSL port.

- 8 Click **Next**. The HPCA Distributed Configuration Server (Destination) Install HPCA Integration Server TCP/IP Port window opens.

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

- Accept the default Integration Server TCP/IP port that is displayed, **3466** (*recommended*); or
- Specify a valid 3- to 5-character decimal Integration Server TCP/IP port.

- 9 Click **Next**. The HPCA Distributed Configuration Server (Destination) Install HPCA Integration Server SSL Port window opens.

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

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



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

- 10 Click **Next**. The HPCA Distributed Configuration Server (Destination) Install Domains window opens.

In this window, specify the domains that will be included in synchronizations between this (Destination) Configuration Server and the Source 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 HPCA Distributed Configuration Server (Destination) Install Enable SSL for window opens.

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

- Click **Enable** or **Disable**.



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

- 12 Click **Next**. The HPCA Distributed Configuration Server (Destination) Install Credentials window opens.

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

- 13 Click **Next**. The HPCA Distributed Configuration Server (Destination) Install Summary window opens. This window displays the directory into which the 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 HPCA Distributed Configuration Server (Destination) Install Finish window opens.

- 15 Click **Finish**. The Destination component of Distributed Configuration Server has successfully installed.

The HPCA Distributed Configuration Server Install Finish window opens.

## 16 Click **Finish**.

Both components of 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 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 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 DCS configuration file, `dmabatch.rc`.

## Setting a Temporary Directory

For each of the DCS 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 Integration Server's root directory. Using the `TMPDIR` parameter in the `/etc/dcs.cfg` configuration file, specify a different location, for example:

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

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

## Destination Component

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

```
array set 0 {
    -temp-dir  c:/cmdcs-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 Configuration Server.



---

## 4 The EDMPROF File and DCS Security

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

- Review the HP Client Automation Configuration Server (Configuration Server) *edmprof file* sections and settings that are relevant to HP Client Automation Distributed Configuration Server (Distributed Configuration Server, DCS) operations.
- Set up *password protection* for DCS synchronizations.

# The EDMPROF File

The `edmprof` file is the text file in which the operational parameters of the Configuration Server are configured and stored. Two of its sections—**MGR\_STARTUP** and **MGR\_DMA**—are integral to enabling DCS and ensuring its proper operation.

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



For a comprehensive look at the `edmprof` file, refer to the *HP Client Automation Configuration Server User Guide (Configuration Server Guide)*.

## Editing the EDMPROF File

The `edmprof` file can be edited in a standard text-editing application.



Be sure to review the important information in this section before editing this file. Failure to do so could adversely effect your HPCA environment.

HP recommends backing up the `edmprof` file prior to editing it.

- You must use a UTF8-aware text editor when editing the `edmprof` file.
- Be sure to select UTF-8 as the *encoding type* when saving the file.
  - Windows users are advised to use **Notepad**.
  - UNIX users are advised to use **vi** or **vim**.

Failure to use a recommended text-editing application and saving the file as recommended in this section could result in the file's changes not being correctly applied to the Configuration Server. This could adversely effect your HPCA environment.

## MGR\_STARTUP Section

The **MGR\_STARTUP** section dictates startup behavior for the Configuration Server. [Table 5](#) on page 47 describes the **MGR\_STARTUP** settings are essential to the operation of the DCS.

**Table 5 MGR\_STARTUP Settings and Values**

| Setting      | Explanation   |
|--------------|---|
| MANAGER_TYPE | In order to ensure that a Configuration Server is DCS-enabled, verify that this value is set to <b>DISTRIBUTED</b> (the default) or <b>SERVER</b> .<br>For additional information, see <a href="#">Configuration Server Eligibility</a> on page 21.   |
| MGR_NAME     | A 32-alphanumeric character (max.) Configuration Server identifier.   |
| MGR_ID       | The unique, 3-digit, hexadecimal ID for a Configuration Server. For more information, see <a href="#">MGR_ID</a> , below. <ul style="list-style-type: none"><li>• DCS uses this value to generate object IDs in the CSDB.</li><li>• Each character in this identifier can have the values 0-9 and A-F.</li></ul> Exception: The 256 consecutive positions from F00 through FFF are reserved for use with Client Automation. |
| TCP_PORT     | The port on which the Configuration Server will listen.<br>This must match the port that is specified for DCS communications ( <code>-master-port</code> in <code>dmabatch.rc</code> ).   |

### MGR\_ID

The MGR\_ID setting establishes a unique identity for each Configuration Server. All Domains in a Configuration Server Database are *owned* by a Configuration Server—identified by the value of MGR\_ID.

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

DCS uses the value of MGR\_ID to determine which 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 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 2](#) on page 15.

## MGR\_DMA Section

In addition to the MGR\_DMA settings that are needed to establish DCS password protection (described in [Configuration Server Security Settings](#) on page 49), there is another DCS-related setting, DMA\_TIMEOUT, which is detailed in [Table 6](#) below.

**Table 6 MGR\_DMA Settings and Values**

| Setting         | Explanation of Value  |
|-----------------|---|
| SECURITY_METHOD | Optional. If not specified, security verification is disabled.<br>To enable native operating system security, specify <b>EDMSIGN</b> .  |
| ADMIN_LIST      | This setting is required if a SECURITY_METHOD is specified.<br>Specify the list of administrators (user IDs) that are allowed to use DCS on this CSDB. The format is a comma-separated (no spaces), case-sensitive list of operating system account names.  |
| DMA_TIMEOUT     | Specify the number of seconds that DCS is to wait for non-DCS tasks to complete before applying a lock to the CSDB. If DCS times out before the task ends, it will abort. The default is <b>0</b> . <ul style="list-style-type: none"><li>• When soft-locking the CSDB, DCS must wait for all administrator tasks to end.</li><li>• When hard-locking the CSDB, DCS waits for all non-DCS tasks to end.</li></ul> |

## Setting up Security

Distributed Configuration Server has an optional security feature that enables an administrator to assign password protection to one or both of the synchronization pair's Configuration Server Databases, 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 CSDBs. DCS defines only one user ID and password. Therefore, all secured CSDBs that 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.

## 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 Configuration Server installation because it is not needed for default operations.

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

### To modify the `edmprof` file

- 1 Stop the Configuration Server.
- 2 Open the `edmprof` file with a UTF8-aware 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 6](#) on page 48.

- 4 Save the changes in UTF8-format, close the `edmprof` file, and restart the 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 Distributed Configuration Server Options and DMABATCH

In this chapter, you will have the opportunity to learn more about:

- The HP Client Automation Distributed Configuration Server (Distributed Configuration Server, DCS) configuration files, `dcs.cfg` and `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.

# Distributed Configuration Server Configuration Files

The Distributed Configuration Server (DCS) uses two configuration files. The `dcs.cfg` file contains settings for the DCS Source. The `dmabatch.rc` file contains settings for the DCS Destination.

## dcs.cfg

This section details the `SNDBUF` parameter, which can be added to the DCS Source configuration file, `dcs.cfg`. To add this option, open `dcs.cfg` in a text editor.

- `SNDBUF` is used to change the DCS network send buffer size (the default is 32K). If you notice slow DCS download or data transfer speeds, you can set this parameter to 64K. For example:

```
dcs::init {
    DBPATH "C:/Program Files/Hewlett-Packard/CM/ConfigurationServer/DB"
    SNDBUF 64K
}
```

- If the TCP window scaling feature is enabled with the TCP window size set to greater than 64K, `SNDBUF` can be increased accordingly (for example: 64K, 128K, or 254K). You can select the size that provides the best performance.

## dmabatch.rc

[Table 7](#) on page 53 describes the settings specified in the DCS Destination configuration file, `dmabatch.rc`. To edit these settings, open `dmabatch.rc` in a text editor.

- All of the options that are important to the basic operation of DCS are populated by values that were specified during the DCS Destination installation programs (see the [Set by Install](#) column in [Table 7](#)). You only need to modify an option when a non-default value is preferred.

In [Table 7](#), the following DCS terminology is used.

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

**Table 7 dmabatch.rc options**

| <b>Option</b>    | <b>Default Value or Required</b> | <b>Set by Install</b> | <b>Description</b>   |
|------------------|----------------------------------|-----------------------|--|
| -master-host     | Required                         | Y                     | IP name/address of the master Configuration Server   |
| -master-id       | Required                         | Y                     | 3 hexadecimal-digit ID of the master Configuration Server                                      |
| -master-port     | Required                         | Y                     | TCP port of the master Configuration Server (usually 3464)                                     |
| -master-ssl-port | 443                              | Y                     | SSL port of the master Configuration Server (usually 443)                                      |
| -master-timeout  | 3600                             | Y                     | Master Configuration Server request timeout (in seconds)                                       |
| -slave-host      | Required                         | Y                     | IP name/address of the slave Configuration Server (local computer name or <i>localhost</i> )   |
| -slave-id        | Required                         | Y                     | 3 hexadecimal-digit ID of the slave Configuration Server                                       |
| -slave-port      | Required                         | Y                     | TCP port of the slave Configuration Server (usually 3464)                                      |
| -slave-ssl-port  | 443                              | Y                     | SSL port of the slave Configuration Server (usually 443)                                       |
| -slave-timeout   | 3600                             | Y                     | Slave Configuration Server request timeout (in seconds)  |
| -http-port       | 3466                             | Y                     | TCP port of the IS (usually 3466)  |
| -https-port      | 444                              | Y                     | SSL port of the IS (often 444; must not be the same as that of <code>-master-ssl-port</code> ) |
| -domains         | “ ” (null)                       | Y                     | Quoted list of blank-separated 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 Configuration Server and/or Integration Server authentication           |

| Option           | Default Value or Required | Set by Install | Description  |
|------------------|---------------------------|----------------|--|
| -password_cipher | AES                       | Y              | TP password-encryption method. Valid values are AES and DES.   |
| -password        | <none>                    | Y              | Password to be used for Configuration Server and/or Integration Server authentication.<br><br>Note: This value can be AES-encrypted or cleartext; it must be consistent with the -password_cipher setting. |
| -dataless        | 0                         | Y              | Skip resources? <b>1</b> =skip resources; <b>0</b> =include resources  |
| -loglvl          | 3                         | Y              | Logging level: <b>3</b> =normal, <b>4</b> =debug, <b>5</b> =debug+   |
| -logfile         | dmabatch.log              | N              | Log file name (no pathing)   |
| -logmode         | w                         | N              | Overwrite the log file? <b>w</b> =overwrite; <b>a</b> =append the log file   |
| -loglines        | 100000                    | Y              | Number of lines to write to the log file before the log rolls over   |
| -logerr          | 1                         | Y              | Echo log to stderr? <b>1</b> =echo; <b>0</b> =don't echo   |
| -logpath         | <none>                    | N              | Override LOGPATH in <code>nvd.ini</code> (location of <code>dmabatch.log</code> )?   |
| -libpath         | <none>                    | N              | Override LIBPATH in <code>nvd.ini</code> (location of client objects)?   |
| -commit          | 1                         | N              | Commit database updates? <b>1</b> =commit; <b>0</b> =don't commit, but remain locked<br><br>See also <a href="#">Deferred Commit</a> on page 60.   |
| -report          | 0                         | N              | Send status-reporting objects to master Configuration Server? <b>1</b> =send; <b>0</b> =don't send   |
| -dmastats-userid | DMA_<id>_<id>_<domains>   | N              | Value of ZUSERID in reporting object, when -report 1.<br><br>Note: For use with the Configuration Server method ZPUTPROF.  |

| Option       | Default Value or Required | Set by Install | Description  |
|--------------|---------------------------|----------------|--|
| -reset       | 0                         | N              | Reset state and unlock Configuration Server on error? 1=reset; 0=leave locked on error   |
| -lock-to     | FAIL                      | N              | Action on pending hard-lock timeout: <b>FAIL</b> , <b>RETRY</b> , or <b>FORCE</b> ?<br>Note: <b>FORCE</b> will kill all non-DCS tasks on slave Configuration Server.                                   |
| -download    | 1                         | N              | A (1   0) toggle that allows you to review the database differences before proceeding with the synchronization. For a more detailed description, see the section, <a href="#">Download</a> below.      |
| -max-deletes | -1                        | N              | A “failsafe” option that can be set in order to prevent the inadvertent deletions of large parts of the database. For more information, see the section, <a href="#">Maximum Deletions</a> on page 56. |

## Download

- If **1**, DCS will download the resources and synchronize the target database.
- If **0**, processing will halt after the Differencing step. The resources are not downloaded and no metadata is committed. If any differences were detected, both databases will remain locked.

Before deciding whether to proceed with the synchronization, check the differences in `zreport.txt`—to see if they are what was expected.

- Any subsequent execution of **dmabatch** without this option, allows the synchronization to resume using the differences that were already generated.
- To abort this synchronization and differencing, run **dmabatch action=reset**.

## Maximum Deletions

An accidental deletion on the master database could be propagated to all the slave databases. This option limits the maximum number of items that can be deleted in one synchronization at the slave database. If the limit is exceeded in the Differencing step, the process is terminated without changing anything. It's up to the user to decide the “reasonable” maximum amount of deletions.

- A value of 0 is valid and will prevent all deletions.
- The default of -1 means no deletion limit.

## Configuration Object Equivalents

Some of the options in `dmabatch.rc` have operational equivalents in the configuration objects `ZMANAGER` and `ZMGRSYNC`. [Table 8](#), below, lists these equivalents.

**Table 8 Configuration object equivalents of dmabatch.rc options**

| Option                       | Set by Install | Configuration Object Equivalent |
|------------------------------|----------------|---------------------------------|
| <code>-master-host</code>    | Y              | <code>ZMANAGER.ZTCPADDR</code>  |
| <code>-master-id</code>      | Y              | <code>ZMGRSYNC.ZSRCMGID</code>  |
| <code>-master-port</code>    | Y              | <code>ZMANAGER.ZTCPPOINT</code> |
| <code>-master-timeout</code> | Y              | <code>ZMANAGER.ZTIMEO</code>    |
| <code>-slave-host</code>     | Y              | <code>ZMANAGER.ZTCPADDR</code>  |
| <code>-slave-id</code>       | Y              | <code>ZMGRSYNC.ZDSTMGID</code>  |
| <code>-slave-port</code>     | Y              | <code>ZMANAGER.ZTCPPOINT</code> |
| <code>-slave-timeout</code>  | Y              | <code>ZMANAGER.ZTIMEO</code>    |
| <code>-domains</code>        | Y              | <code>ZMGRSYNC.ZDOMAINS</code>  |
| <code>-userid</code>         | Y              | <code>ZMGRSYNC.BATUSER</code>   |
| <code>-password</code>       | Y              | <code>ZMGRSYNC.BATPWD</code>    |
| <code>-dataless</code>       | Y              | <code>ZMGRSYNC.NORES</code>     |
| <code>-report</code>         | N              | <code>ZMGRSYNC.REPORT</code>    |



| Option           | Set by Install | Configuration Object Equivalent |
|------------------|----------------|---------------------------------|
| -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 **EDMPPRO**



Each execution of 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 9 below defines the fields of the DMASTATS object.

**Table 9 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)<br><b>Notes:</b> See <a href="#">Table 10</a> on page 58 for REPORTID values.<br>See <a href="#">Table 11</a> on page 59 for detailed BATCHRC information. |

| Field     | Definition  |
|-----------|---|
| BATCHMSG  | Completion message (if REPORTID > 1)<br><b>Note:</b> See <a href="#">Table 10</a> below for REPORTID values.  |
| BATARGS   | DMABATCH command line   |
| BATLKSTA  | Result of <b>DMABATCH ACTION=LOCKSTATUS:</b><br><b>U</b> (Unlocked); <b>S</b> (Soft-locked); <b>X</b> (Exclusive Soft-locked); <b>H</b> (Hard-locked) |
| DMASTATE  | <b>0</b> = Initial; <b>1</b> = Compared; <b>2</b> = Downloaded; <b>3</b> = Committed  |
| ZSRCMGRID | -master-id (Source MGR_ID)  |
| ZDSTMGRID | -slave-id (Destination MGR_ID)  |
| REPORTID  | Identifies which DCS processing point sent the report.<br><b>Note:</b> See <a href="#">Table 10</a> below for detailed REPORTID information.          |
| SCOPE     | N/A   |
| ZDOMAINS  | List of domains   |
| ZUSERID   | User name for use with PUTPROF method (see <a href="#">ZUSERID</a> on page 59)  |

[Table 10](#) below identifies which DMASTATS.REPORTID processing point sent the report.

**Table 10 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 11](#) on page 59 lists the Configuration Server BATCHRC and corresponding BATCHMSG responses to DCS requests.

**Table 11 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     | Configuration Server 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 Configuration Servers locked. If leaving both 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 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

DCS offers the ability to defer committing the database updates on the Destination 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 Configuration Server is less busy, specify:

**DMABATCH COMMIT=NO**

All 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 Configuration Server will be unlocked,
- Destination Configuration Server will be soft-locked.

To commit the database updates to the Destination 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-DCS HPCA agent tasks from starting.
- **QTYPE=TRANS**: same as **TASK**, but also, for currently running non-DCS HPCA agent tasks, the HPCA agent connection terminates when the HPCA 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 DCS to enter the Commit phase. It terminates all non-

DCS HPCA agent tasks on the Destination, allowing a 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 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 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 Configuration Server will be hard-locked, thereby preventing HPCA agents from connecting. Also, any HPCA agent tasks that are running on the Configuration Server are killed.

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



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

## CSID Value Considerations

- If **CSID=** is omitted, the default is the Destination Configuration Server's ID.
- If **CSID ≠** the Source or Destination Configuration Server (master or slave), the **-port** and **-address** of the 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 11](#) on page 59), 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 DCS, the 000 return code indicates that the phase was successful.

The corresponding BATCHMSG is “Successfully Completed.”





# A Troubleshooting the Distributed Configuration Server

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

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



If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started and Concepts Guide* as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

## Logs to Obtain

For Distributed Configuration Server problems, `dmabatch.log` and the Destination Configuration Server log are needed. Although, it is unlikely that the Source 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 Configuration Server.

**Table 12 Domain eligibility error messages**

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

## Log and Object Locations

The default locations for the 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 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 Distributed Configuration Server.

## Distributed Configuration Server Objects and Files

### Distributed Configuration Server Objects

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

- `ZMANAGER` contains the properties of all the Configuration Servers that have been defined to DCS. TP parameters (including TP trace level) are defined here, per 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 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 11](#) on page 59.



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

### Distributed Configuration Server Files

This section defines the 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 Configuration Servers.

## .DAT

These files cache a domain's *small resource* files. This is a performance feature that minimizes CSDB file operations.

- .DAT files are built on Solaris and Windows platforms only; on Source 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 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 CSDB objects.



For more information on the EDMAMS verbs, refer to the *HP Client Automation Configuration Server User Guide (Configuration Server Guide)*.

The EDMAMS verb `UPDATE_MGRIDS` can be used to update the `MGR_ID`, Configuration Server name, owning `MGR_ID`, and owning 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 Configuration Server name) (,MID=local Configuration Server ID) (,MMNAME=owning Configuration Server name) (,MMID=owning Configuration Server ID)
```

## Domain Eligibility

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

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



Refer to the *Configuration Server Guide* for more information about the **MANAGER\_TYPE** setting of the **MGR\_STARTUP** section of the `edmprof` file.



# Index

.

.dat files, 68

.idx files, 68

.mk files, 68

## A

Admin CSDB Editor, 25

Admin Packager, 25

Admin Publisher, 25

ADMIN\_LIST, 48, 50

## B

BATCHMSG, 58

BATCHRC, 58, 62

BATCHRC and BATCHMSG values, 59

## C

Configuration Server

destination, 21

security, 49

source, 20

synchronization eligibility, 21

synchronization pair, 21

configuring Distributed Configuration Server, 26

container file, 16

Core servers, 19

CSDB Editor. *See* Admin CSDB Editor

current MGR\_ID, 22

## D

Database Editor. *See* Admin CSDB Editor

Destination component, 21

installation, 37

temporary directory, 43

Destination Configuration Server, 21

defined, 15

MANAGER\_TYPE setting, 22

DISTRIBUTED, 21

SERVER, 21

performance improvements, 22

directories, Distributed Configuration Server, 31

Distributed Configuration Server

batch mode, 26

communications protocol, 30

configuring, 26

defined, 15

description, 18

Destination component installation, 37

Destination Configuration Server, 20

directories, 31

domain eligibility rules, 25

log error messages, 66

installation

Destination component, 37

Source component, 34

installation options, 30

Destination component, 30

Source component, 30

logs, 26, 66

Configuration Server logs, 66

DMABATCH.LOG, 66

log error messages, 66

objects, 26

saved, 67

ZMANAGER, 67

ZMGRSYNC, 67

processor requirements, 30

saved objects, 67

security, 48

password, 49

setting up, 48

settings, 49

user ID, 49

- Source component installation, 34
- Source Configuration Server, 20
- space requirements, 32
- system requirements, 30
- terminology, 14
  - container file, 16
  - Destination Configuration Server, 15
  - domain ownership, 15
  - foreign-owned domain, 15
  - middle-tier Configuration Server, 16
  - peer synchronization, 15
  - self-owned domain, 15
  - Source Configuration Server, 15
  - synchronization, 15
  - synchronization pair, 15
  - unrelated domains, 16
- DMA\_TIMEOUT, 48
- DMABATCH
  - hardlock, 62
  - kill tasks, 62
  - quiesce, 61
  - reset, 62
  - resume, 61
  - softlock, 62
  - unlock, 62
- dmabatch.exe, 26
- DMABATCH.LOG, 66
- dmabatch.rc options, 53
- DMASTATS, 57
  - BATCHRC, 58
  - fields defined, 57
  - REPORTID, 58
- document map, 14
- domain eligibility, 25
  - error messages, 66
  - rules, 25
    - domain deletion, 25
- domain naming considerations, 23
- domain ownership, 22
  - defined, 15
  - establishing, 22
- domains

- current MGR\_ID, 22
- domain name, 22
- eligibility, 25
  - rules, 25
- foreign-owned, 23
- local updates, 26
- owning MGR\_ID, 22
- self-owned, 22
- unrelated, 26

## E

- Editor. *See* Admin CSDB Editor
- EDMAMS, 68
  - UPDATE\_MGRIDS, 69
- edmprof file, 46, 49
  - MGR\_DMA, 48
  - MGR\_STARTUP, 21, 22, 46
  - MGR\_TRACE, 67
- EDMSIGNR, 49
- eligibility, domains, 25

## F

- files
  - .dat, 68
  - .idx, 68
  - .mk, 68
- foreign-owned domain, 23
  - defined, 15

## H

- hardlock Source Configuration Server Database, 62
- HPCA Core, 14, 29, 65
- HPCA Satellite, 14, 29, 65

## I

- IDMLIB, 66
- IDMLOG, 66
- installing
  - Destination component, 37
  - Distributed Configuration Server, 32
  - Source component, 34



- Integration Server, 20, 43
  - defined, 15
- internet protocol addressing structure, 19
- IP Networking Support, 19
- IP version 4, 19
- IP version 6, 19
- IPv4, 19
- IPv6, 19

## K

- kill (non-DCS HPCA agent) tasks, 62

## L

- local updates, 26
- logs
  - synchronization, 26

## M

- MANAGER\_TYPE setting, 21
  - performance improvements, 22
  - using to improve performance, 22
- MGR\_DMA, 46, 48, 49
  - ADMIN\_LIST, 48
  - DMA\_TIMEOUT, 48
  - SECURITY\_METHOD, 48, 49
- MGR\_ID, 22, 47
- MGR\_STARTUP, 46
  - MANAGER\_TYPE, 21, 47
  - DISTRIBUTED vs. SERVER, 21, 22
  - MGR\_ID, 47
  - MGR\_NAME, 47
  - TCP\_PORT, 47
- MGR\_TRACE, 67
- middle-tier Configuration Server, 18, 22
  - defined, 16
  - MANAGER\_TYPE setting, 22
  - SERVER, 22
  - performance improvements, 22

## O

- owning MGR\_ID, 22

## P

- Packager. *See* Admin Packager
- peer synchronization, 18
  - defined, 15
- platform support, 30
- Portal, 21
- pre-installation notes, UNIX, 32
- processor requirements
  - Distributed Configuration Server, 30
  - Proxy Server, 21
- Publisher. *See* Admin Publisher
- PUTPROF, 57

## Q

- quiesce
  - Destination Configuration Server Database, 61
- quiesce, qtype, 61
  - task, 61
  - trans, 61

## R

- REPORTID, 58
  - values defined, 58

## S

- Satellite servers, 19
- saved Distributed Configuration Server objects, 67
- security
  - Configuration Server, 49
  - Distributed Configuration Server, 49
- SECURITY\_METHOD, 48, 49
- self-owned domain, 22
  - defined, 15
- simultaneous synchronizations, 27

- softlock Source Configuration Server Database, 62
- source component, 20
  - installation, 34
  - temporary directory, 43
- Source Configuration Server, 21
  - defined, 15
  - MANAGER\_TYPE setting, 21
    - DISTRIBUTED, 21
    - SERVER, 21
- supported platforms, 30
- synchronization
  - defined, 15
  - domain eligibility, 25
  - logs, 26
  - reset, 62
  - resume, 61
  - simultaneous, 27
- synchronization pair, 21
  - control information, 19
  - defined, 15
  - ZMGRSYNC, 67
- system requirements, 30

## T

- temp-dir, 43
- temporary directories, 42
  - Destination, 43
  - Source, 43
  - temp-dir, 43
  - TMPDIR, 43
- terminology, 14
- TMPDIR, 43

- troubleshooting Distributed Configuration Server
  - Configuration Server property information, 67
  - Distributed Configuration Server logs, 66
  - domain eligibility, 69
  - EDMAMS utility, 68
    - UPDATE\_MGRIDS, 69
  - files
    - .dat, 68
    - .idx, 68
    - .mk, 68
  - IDMLIB, 66, 67
  - IDMLOG, 66
  - INI files, 66
  - no eligible domains, 69
  - synchronization pair information, 67
  - tracing, 67

## U

- UNIX pre-installation notes, 32
- unlock Source Configuration Server Database, 62
- unrelated domains, 26
  - defined, 16

## Z

- zedmams. *See* EDMAMS
- ZMANAGER, 67
  - Configuration Server property information, 67
- ZMGRSYNC, 67
  - BATCHMSG, 63
  - BATCHRC, 63
  - Distributed Configuration Server sessions saved, 67
  - synchronization pair saved, 67
- ZUSERID, 58, 59