

# HP OpenView Distributed Configuration Server Using Radia

for the HP-UX, Linux, Solaris, and Windows operating systems

Software Version: 4.7.1

---

## Installation and Configuration Guide

Manufacturing Part Number: T3424-90092

June 2005



## Legal Notices

### Warranty

*Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.*

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

### Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company  
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

### Copyright Notices

© Copyright 1998-2005 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

### 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.

### Acknowledgements

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

## Support

Please visit the HP OpenView support web site at:

**<http://www.hp.com/managementsoftware/support>**

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

HP OpenView 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 valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

**[http://www.hp.com/managementsoftware/access\\_level](http://www.hp.com/managementsoftware/access_level)**

To register for an HP Passport ID, go to:

**<http://www.managementsoftware.hp.com/passport-registration.html>**

# Revisions

## Version Differences

- ▶ This section has been included for the benefit of existing Distributed Configuration Server customers.

This version of the Installation and Configuration Guide for the HP OpenView Distributed Configuration Server Using Radia (Distributed Configuration Server Guide) contains several performance, operational, and user-interface differences from previous versions. These differences include the addition of some features and options, and the removal of others, as detailed in the following table.

**Table 1: Differences in Version 4.7**

Change	Description
User Interface	<p>In 4.7.1 there is a scaled-back user interface, with which an administrator of HP OpenView Using Radia can only configure Distributed Configuration Server synchronizations. This interface is the file, <code>dcs.exe</code>, and it must be installed on any Configuration Server that will act as Destination.</p> <p>Once the Destination component is installed, an invocation option (called Configuration) can be accessed by navigating through the <b>Start</b> menu (and optionally from a desktop icon called <b>RDCS Configuration</b>). See Installing the Distributed Configuration Server starting on page 39.</p> <p>Note: This configuration-only interface cannot be invoked from a command line.</p>

Change	Description
Executables	<p>In 4.7.1 the Distributed Configuration Server Batch executable is <code>dmabatch.exe</code>, aligning it with version 4.5. See Chapter 7, Distributed Configuration Server's DMABATCH.</p> <p>Note: Customers that have been scripting Distributed Configuration Server with version 4.6 will need to make this adjustment from <code>dcsbatch.exe</code>.</p>
Differencing	<p>The tree-differencing feature that was introduced in 4.6 is not supported in 4.7.</p> <p>See Chapter 6, Configuring Distributed Configuration Server Options.</p> <p>The control differencing vs. CRC differencing choice in earlier versions is superseded by a single, new differencing method in version 4.7.</p> <p>See Chapter 6, Configuring Distributed Configuration Server Options.</p>
Patching	<p>The byte-level differencing (BLD) patching feature that was introduced in version 4.6 (activated with the <b>Build Resources by Patching</b> check box on the <b>Staging</b> tab) is not supported in version 4.7.</p> <p>See Chapter 6, Configuring Distributed Configuration Server Options.</p>
Pre-Staging	<p>The external pre-staging feature, introduced in version 4.6 (the <b>External Staging Location</b> field of the Staging tab), is not supported in version 4.7.</p> <p>See Distributed Configuration Server Processes Defined, starting on page 31.</p>
Database Verification	<p>The pre-synchronization database-verification feature that was optional in version 4.6 (enabled with the <b>Verify control data (pre-sync)</b> check box on the Batch Operation tab) is not selectable because it is permanently active in version 4.7.</p> <p>See Batch Operation Options, starting on page 96.</p>

<b>Change</b>	<b>Description</b>
Lock Exposure	The <b>Batch Lock Exposure Action</b> option which, in version 4.6 on the Batch Security tab, could be set to <b>Continue</b> , <b>Reset</b> , or <b>Continue if DB unchanged</b> , is, in version 4.7.1, hard-coded to <b>Continue if DB unchanged</b> . See Batch Security Options, starting on page 97.
Integration Server	In version 4.7.1, the Source component of Distributed Configuration Server (which contains the Integration Server—HP OpenView Using Radia's HTTP server) must be co-resident with any Configuration Server that will be a master in a Distributed Configuration Server synchronization. See Source Component, starting on page 23.
Co-Residency	In version 4.7.1, the Destination component of Distributed Configuration Server ( <code>dmabatch.exe</code> ) must be co-resident with any Configuration Server that will act as destination in a Distributed Configuration Server synchronization. See Destination Component, starting on page 24.
COMMIT=NO	In version 4.7.1, if the COMMIT=NO command-line option is specified, and the synchronization is reset without the commit being done (as specified), resource orphans for the added resources might be left in the Destination database. Note: This behavior was not present in 4.6 because COMMIT=NO allowed the synchronization to be done in two phases, at different times of day, but did not allow a partial synchronization. See Deferred Commit, starting on page 106.

<b>Change</b>	<b>Description</b>
Lost & Found	<p>In version 4.6, the goal was to accurately replicate databases, even if it meant replicating logical database errors. In 4.7.1, the intent is beyond simple replication—rather, it is the creation of a verifiable Destination database.</p> <p>Note: In 4.7.1, database items that can be identified as being “in-error” or inconsistent, such as resource orphans, will be placed into a new directory, <code>lost+found</code>, under the Destination database root, instead of being placed in the Destination database. The result should then pass the database verification.</p> <p>See Distributed Configuration Server Processes Defined, starting on page 31.</p>



# Product Changes

## Version 4.7.1

This version of the HP OpenView Distributed Configuration Server Using Radia features the addition of Linux support.

## Documentation Changes

This printing of the Distributed Configuration Server Guide contains the following changes to information and procedures.

### Chapter 3: Installing the Distributed Configuration Server

- Page 37, Supported Operating Systems is a new section.
- Page 37, Distributed Configuration Server Directories is a new section.
- Page 39, the section Installing the Distributed Configuration Server, was revised.
- Page 63, Setting a Temporary Directory is a new section.

### Appendix A: Troubleshooting the Distributed Configuration Server

- Page 112, the section Log Error Messages was revised.
- Page 113, the section Distributed Configuration Server Objects and Files was revised and renamed.
- Page 114, Distributed Configuration Server Files is a new section.



# Contents

Revisions .....	5
Version Differences.....	5
Product Changes.....	9
Version 4.7.1.....	9
Documentation Changes .....	9
Chapter 3: Installing the Distributed Configuration Server .....	9
Appendix A: Troubleshooting the Distributed Configuration Server .....	9
1 Introduction .....	15
Documentation Map .....	16
Terminology .....	17
2 Introduction to the Distributed Configuration Server.....	21
Overview.....	22
Distributed Configuration Server.....	22
Distributed Configuration Server Components .....	23
Source vs. Destination.....	23
Two Configuration Servers: A Synchronization Pair .....	24
Configuration Server Eligibility.....	25
Domain Ownership.....	25
Domain Naming Considerations .....	26
One Owner vs. Multiple Owners.....	26
One Owning Configuration Server .....	26
Multiple Owning Configuration Servers.....	27
Domain Eligibility .....	28
Selecting Domains .....	28
Domain Eligibility Rules .....	28

Distributed Configuration Server Configuration .....	30
Distributed Configuration Server: Batch Mode .....	30
Synchronization Logs .....	30
Simultaneous Synchronizations.....	30
Distributed Configuration Server Planning.....	31
When to Use Distributed Configuration Server .....	31
Distributed Configuration Server Processing .....	31
Distributed Configuration Server Processes Defined .....	31
<b>3 Installing the Distributed Configuration Server.....</b>	<b>35</b>
Two-Phase Installation .....	36
Recommendations and Requirements.....	36
Supported Operating Systems .....	37
Distributed Configuration Server Directories.....	37
Source .....	38
Destination.....	38
Distributed Configuration Server Space Requirements.....	39
Installing the Distributed Configuration Server.....	39
UNIX Pre-Installation Notes .....	39
Installing the Distributed Configuration Server Source Component.....	43
Installing the Distributed Configuration Server Destination Component .....	49
Setting a Temporary Directory .....	63
Source Component .....	63
Destination Component.....	63
<b>4 Distributed Configuration Server Security .....</b>	<b>65</b>
Setting up Security.....	66
Native Operating-System Security .....	66
Enabling Native Operating-System Security .....	66
Configuration Server Security Settings .....	68
<b>5 Setting Up a Distributed Configuration Server Synchronization ....</b>	<b>71</b>
Configuration Servers in Distributed Configuration Server .....	72

Adding Configuration Servers.....	72
Copying Configuration Servers.....	75
Deleting Configuration Servers.....	76
List of Configuration Servers.....	76
Distributed Configuration Server Configuration .....	77
Navigation Buttons and Menu Options.....	77
Navigation Buttons .....	77
Menu Options.....	77
Configuration Mode Panels .....	78
Configuration Server Definition Panel .....	78
Choose Configuration Servers and Domains Panel.....	80
Choosing Configuration Servers and Domains.....	82
The Configuration Server's EDMPROF File.....	84
MGR_STARTUP Section.....	84
MGR_DMA Section.....	85

## 6 Configuring Distributed Configuration Server Options ..... 87

Distributed Configuration Server Options.....	88
General Options .....	88
DMASTATS.....	91
ZUSERID .....	93
Differencing Options .....	94
Staging Options.....	95
Batch Operation Options .....	96
Batch Security Options.....	97

## 7 Distributed Configuration Server's DMABATCH ..... 101

Overview.....	102
DMABATCH Considerations.....	102
DMABATCH Scripting Commands.....	102
DMABATCH Line Commands .....	103
DMABATCH Automation .....	104
Automated Solutions.....	105
Reset Session on Staging Failure .....	105

Batch Lock Timeout Action.....	106
DMABATCH Command-Line Options.....	106
Deferred Commit .....	106
IP Address Support for Cloned Managers .....	107
Hard-lock Operation.....	107
Results of DMABATCH .....	108
Configuration Server Response to Distributed Configuration Server Request .....	108
<b>A Troubleshooting the Distributed Configuration Server.....</b>	<b>111</b>
Logs to Obtain.....	112
Log Error Messages .....	112
Log and Object Locations .....	113
Configuration Server Tracing for Distributed Configuration Server.....	113
Distributed Configuration Server Objects and Files.....	113
Distributed Configuration Server Objects.....	113
Distributed Configuration Server Files .....	114
The EDMAMS Utilities .....	115
Domain Eligibility .....	116
<b>Index.....</b>	<b>117</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 OpenView Distributed Configuration Server Using Radia (Distributed Configuration Server)
- Become familiar with some of the HP OpenView Using Radia terminology
- Become familiar with some of the Distributed Configuration Server-specific HP OpenView Using Radia terminology

# Documentation Map

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

**Table 2: Document Map**

<b>Chapter</b>	<b>Contents</b>
Chapter 2 Introduction to the Distributed Configuration Server	Distributed Configuration Server, including: how Distributed Configuration Server works; the roles of the two Distributed Configuration Server components; Configuration Server eligibility, domain ownership and domain eligibility.
Chapter 3 Installing the Distributed Configuration Server	Installing the two Distributed Configuration Server components, including: system recommendations and desktop shortcut icons.
Chapter 4 Distributed Configuration Server Security	Setting up security for Distributed Configuration Server, including: password protection on the host operating system.
Chapter 5 Setting Up a Distributed Configuration Server Synchronization	Defining Configuration Servers to Distributed Configuration Server, including: specifying their properties; and choosing a synchronization pair.
Chapter 6 Configuring Distributed Configuration Server Options	Configuring Distributed Configuration Server, including: a detailed look at the various Distributed Configuration Server settings that are available on the various Options tabs.
Chapter 7 Distributed Configuration Server's DMABATCH	Executing a Distributed Configuration Server session on a command-line, including: scripting, and automation and command-line options.



Chapter	Contents
Appendix A Troubleshooting the Distributed Configuration Server	Troubleshooting Distributed Configuration Server, including: logs, tracing, and domain eligibility

## Terminology

The following table lists the terms that might be used interchangeably throughout this book, as well as in other HP OpenView Using Radia publications.



Substitution is dependent on the context and, therefore, is not always possible.

**Table 3: Terminology**

Term	Alternate
Application	software, service
Client	Radia client, Application Manager, Software Manager
Computer	workstation, server, machine, host
edmprof file	Configuration Server Settings File; Profile File; Profile Editor; edmprof.dat (Windows); .edmprof (UNIX) Note: This is the text file wherein a Configuration Server's operational parameters are specified. This manual uses this non-platform specific, generic reference.
NOVADIGM domain	PRDMAINT domain Note: Starting with the 4.0 release of the Radia database, the NOVADIGM domain was renamed to PRDMAINT. Therefore, references to the PRDMAINT domain can be assumed to be referencing the NOVADIGM domain in pre-version 4.0 Radia databases.
Configuration Server	Manager, Active Component Server

Table 4 describes the Distributed Configuration Server-specific terms that are used in this document. It is recommended that you review these terms and their descriptions in order to better understand the concepts and materials contained herein.

**Table 4: Distributed Configuration Server Terminology**

<b>Term</b>	<b>Description</b>
Distributed Configuration Server	Formerly known as EDM DMA, the Distributed Configuration Server is an extension of the Configuration Server. It synchronizes Radia databases that are running on separate (Distributed Configuration Server-enabled) machines across an enterprise.
Integration Server	The HTTP file server of HP OpenView Using Radia. 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	In a Distributed Configuration Server synchronization, the Configuration Server that houses the <b>master</b> Radia database.
Destination Configuration Server	In a Distributed Configuration Server synchronization, the Configuration Server that houses the Radia database that is the <b>target</b> . Note: This is <i>always</i> a replica of the Source database.
Synchronization	The act of replicating a master Radia database (Source) on a target Radia database (Destination).
Peer Synchronization	Synchronizing a domain on a Destination Configuration Server from a Source Configuration Server that does not own the domain. See Foreign-Owned Domain in this table.
Synchronization Pair	Two Configuration Servers that have been configured (as Source and Destination) for synchronization.
Domain Ownership	All domains must be “owned” by a Configuration Server. Domains are either <b>self-owned</b> or <b>foreign-owned</b> .

<b>Term</b>	<b>Description</b>
Self-Owned Domain	A domain that is owned by the current Configuration Server. Ownership is established at installation, or when a domain is added to the database. 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. Note: If the owning MGR_ID and current MGR_ID are different, the domain is foreign-owned.
Unrelated Domains	Domains that are not owned by the same Configuration Server—that is, they do not have the same owning MGR_ID.
Middle-tier Configuration Server	A middle-tier Configuration Server is defined to more than one Distributed Configuration Server agent in order to affect changes across Configuration Servers that lack communications access to a single Distributed Configuration Server agent.
Cloned Manager	Cloned Managers are Configuration Servers that share a database and a MGR_ID. They are distinguishable only by their IP name/address. Note: The database is “owned” by only one of the Configuration Servers, which can update and synchronize it.
Container File	A file, created on the Source, in which the instance data is compressed before being transferred to the Destination. This file is much faster to transfer than a large number of small files. Note: At the Commit phase, the instance-container file is used as the data source, so the files are moved directly from it to their ultimate destination. This minimizes the number of times that the data is moved and the length of time that the Radia database is hard-locked.



## 2 Introduction to the Distributed Configuration Server

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

- How the Distributed Configuration Server works to synchronize Radia 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 Configuration Servers for synchronization, based on Configuration Server *eligibility* and *domain ownership*
- The role of Radia database domains in Distributed Configuration Server operations, as well as: *domain-naming considerations*, *domain eligibility*, and *selecting domains*
- How to establish *domain ownership across the enterprise*, and how to use this to set up *simultaneous synchronizations*
- The *steps of the Distributed Configuration Server process*, which will aid in troubleshooting

## Overview

The Distributed Configuration Server is a powerful tool that enables you to efficiently manage multiple Configuration Servers in a networked environment. Using the Distributed Configuration Server, an administrator can share information about policies and managed applications across numerous Configuration Servers, thereby improving the scalability, flexibility, and extensibility of the environment.

## Distributed Configuration Server

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

► Additional Distributed Configuration Server *dependency*, *directory*, and *requirement* information is presented in the sections Supported Operating Systems, starting on page 37 and Distributed Configuration Server Directories, starting on page 37.

For more information on the functionality of the Distributed Configuration Server components, see the section, Distributed Configuration Server Components starting on page 23.

In a multi-tier configuration, both components can be installed on the same machine in order to accommodate *peer synchronizations* and *middle-tier Configuration Server* capabilities. Peer synchronizations and middle-tier Configuration Servers are defined in Table 4 on page 18.

Distributed Configuration Server is designed to synchronize Distributed Configuration Server-enabled Radia databases throughout an enterprise so, although it is not essential that the Radia databases directly communicate with one another, Distributed Configuration Server must be able to communicate with both Configuration Servers that comprise the synchronization pair (see Two Configuration Servers: A Synchronization Pair on page 24).

In a synchronization operation, Distributed Configuration Server compares the control information of one Radia database with that of another, for the domains that have been selected.

## Distributed Configuration Server Components

Inasmuch as there are two Configuration Servers involved in Distributed Configuration Server synchronizations, the two Distributed Configuration Server 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 Distributed Configuration Server *Source* component installed.
- Similarly, each Configuration Server that will act as a Destination must have the Distributed Configuration Server *Destination* component installed.
- If a Configuration Server has both components of the Distributed Configuration Server installed, it can act as Source and Destination, albeit in separate Distributed Configuration Server operations.

With the Distributed Configuration Server components installed on the Configuration Server machines, Distributed Configuration Server:

- 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 HP OpenView Integration Server Using Radia (Integration Server), the product suite's HTTP server.



### Integration Server Notes

- For a brief description of Integration Server and how it relates to Distributed Configuration Server, see the section, Integration Server.
- For a detailed description of Integration Server, refer to the *Essentials Guide for HP OpenView Using Radia (Essentials Guide)*, available in the HP OpenView Using Radia 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 Radia database instance.

### Integration Server

Integration Server is the HP OpenView Using Radia 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 4 starting on page 18).

Integration Server is not a separately licensed HP product. It integrates several independent modules (HP OpenView Management Portal Using Radia [Management Portal], HP OpenView Proxy Server Using Radia [Proxy Server], HP OpenView Inventory Manager Using Radia [Inventory Manager]) 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 Distributed Configuration Server 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*. In order for a Configuration Server to be part of a synchronization pair, it must be defined to the Distributed Configuration Server component on the



Destination Configuration Server, as described in the section, Configuration Servers in Distributed Configuration Server, starting on page 72.

Distributed Configuration Server 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 Distributed Configuration Server 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 Distributed Configuration Server operation, a Configuration Server must meet the following requirements.

- In its `edmpprof` file it must be Distributed Configuration Server-enabled. This is done by specifying:

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



By default, all Configuration Servers are installed as DISTRIBUTED.

- It must have either the Distributed Configuration Server Source or Destination component installed.

## Domain Ownership

Radia database domains on each Configuration Server have three distinguishing characteristics: **domain name**, **owning MGR\_ID**, and **current MGR\_ID**.



For planning purposes, we recommend maintaining unique names for Radia database domains.

- A self-owned domain is a Radia database 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 Radia database domain that is owned by a Configuration Server other than the current one, and which is present as the result of a Distributed Configuration Server 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 the section, Distributed Configuration Server Planning, starting on page 31.

## One Owning Configuration Server

Table 5 lists the benefits and drawbacks of one Configuration Server owning all the domains.

**Table 5: 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 RADIUS database to backup	Does not align well with highly de-centralized organizations
Data flow throughout the environment is one-way	Data flow throughout Distributed Configuration Server is one-way
Aligns with highly centralized organizations	

### Multiple Owning Configuration Servers

Table 6 lists the benefits and drawbacks of domain ownership being assigned to multiple Configuration Servers.

**Table 6: Multiple Domain-Owning Configuration Servers**

<b>Advantages</b>	<b>Disadvantages</b>
Aligns readily with highly de-centralized 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 Distributed Configuration Server 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 last synchronization for the synchronization pair, or
- The last update with HP OpenView Using Radia administrative components (such as HP OpenView System Explorer Using Radia [System Explorer], HP OpenView Packager Using Radia [Packager], and HP OpenView Publisher Using Radia [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 Distributed Configuration Server 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 Distributed Configuration Server domain synchronization eligibility rules are listed below. These apply to each domain independently. See Log Error Messages on page 112.

- 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 Distributed Configuration Server 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 HP OpenView Using Radia component, it cannot be used as the Source in a *peer synchronization*.
  - ▶ A local update occurs when a database is updated via an HP OpenView Using Radia component (such as System Explorer, Publisher, and Packager) other than Distributed Configuration Server.
- When it is possible to make such a distinction, the Distributed Configuration Server 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.

# Distributed Configuration Server Configuration

Distributed Configuration Server functionality must be configured for two Configuration Servers. The Configuration Servers must be defined to Distributed Configuration Server, as described in the section, Configuration Servers in Distributed Configuration Server, on page 72. After the Configuration Servers have been defined, the synchronization pair and eligible domains must be selected, as described in the section, Choosing Configuration Servers and Domains, on page 82.

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

## Distributed Configuration Server: Batch Mode

The command-line, or **batch**, mode of Distributed Configuration Server is invoked by the executable, `DMABATCH.EXE`, which can be triggered via the desktop icon, **RDCS Batch**. Once the synchronization is started, it will execute “under-the-covers,” with no further administrator action required. This is discussed in further detail in Chapter 7, Distributed Configuration Server’s DMABATCH.

## 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 only the most recent run of Distributed Configuration Server.

## 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 Distributed Configuration Server would prove beneficial.

- To replicate Radia database contents across an enterprise.
- When moving domains from a test environment to a production environment.
- As an alternative to local connects.

Developing a viable, functional Distributed Configuration Server infrastructure requires knowledge of:

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

## Distributed Configuration Server Processing

Although the Distributed Configuration Server runs under-the-covers after the graphical configuration, it is helpful to know the processing that takes place after the synchronization has begun. This knowledge will aid in troubleshooting and problem resolution. The following section, Distributed Configuration Server Processes Defined, describes the Distributed Configuration Server processes.

### Distributed Configuration Server Processes Defined

This section describes the Distributed Configuration Server processes, including the lock status of the Radia database on the Source and Destination.

### **Task 1** Define Configuration Servers

Configuration Servers are defined (added, copied, and deleted) for Distributed Configuration Server.

During this phase, the Source and Destination databases are unlocked—they are fully accessible to all HP OpenView Using Radia components to which they are defined.

### **Task 2** Select Configuration Servers and domains to be synchronized

The synchronization pair and eligible domains are selected.



The synchronization pair's property information is saved in the ZMANAGER object on the Destination Configuration Server.

The synchronization information is saved in the ZMGRSYNC object on the Destination Configuration Server.

Note: This synchronization pair will stay defined to Distributed Configuration Server until a new synchronization pair is selected.

The list of eligible domains is dynamically created based on the:

- Synchronization pair
- Database control information for the last synchronization, or update from an HP OpenView Using Radia component.

During this phase, the Source and Destination databases are unlocked—they are fully accessible to all HP OpenView Using Radia components to which they are defined.



The next three steps run “under the covers” in the batch mode, DMABATCH.

### **Task 3** Difference the Source and Destination control data

The database instances are packed into the container file, which is compressed.

Distributed Configuration Server uses instance list retrieval and differencing to detect only those database changes that are made with HP OpenView Using Radia components.

- The only exception to this is if an entire domain is deleted.





Class and instance modifications, additions, and deletions should be done at the Source (owning) database only, because during synchronization, Distributed Configuration Server will use domain information from the Source causing any changes that were made at the Destination to be overwritten.

During this phase, both databases are soft-locked—they are read-only to other HP OpenView Using Radia components to which they are defined.

#### **Task 4** Download and Transfer the Data Resources from the Source

The container file is transferred from the Source to the Destination, and the instance data is written directly to its ultimate location—but with a special file extension in order to avoid overlaying.

During this phase, both databases are soft-locked—they are read-only to other HP OpenView Using Radia components to which they are defined .

#### **Task 5** Commit the changes to the Destination Configuration Server

The database changes that were discovered as a result of the synchronization are committed to the Destination database.

During this phase, the Source database is unlocked and the Destination is hard-locked. This means that the Source is fully accessible to all HP OpenView Using Radia components, but there is no reading from or writing to the Destination until the commit is finished.



---

## 3 Installing the Distributed Configuration Server

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

- Successfully installed the Distributed Configuration Server **Source** component
- Successfully installed the Distributed Configuration Server **Destination** component

## Two-Phase Installation

In order to set up a “distributed” Configuration Server synchronization environment, Distributed Configuration Server enables an HP OpenView Using Radia administrator to install:

- The Distributed Configuration Server Source component,
- The Distributed Configuration Server Destination component, or
- Both Distributed Configuration Server components.

The installations are outlined in the section, Installing the Distributed Configuration Server, starting on page 39.

- The Distributed Configuration Server Source component must be installed on any Configuration Server whose database is going to be the master in Distributed Configuration Server synchronization.
- The Distributed Configuration Server Destination component must be installed on any Configuration Server that is going to be the target in Distributed Configuration Server synchronization.



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

For a detailed description of these components, see the sections, Source Component and Destination Component starting on page 23.

## Recommendations and Requirements

To ensure the successful installation and operation of the HP OpenView Distributed Configuration Server Using Radia, the following system requirements are recommended.

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

## Supported Operating Systems

Both components of the Distributed Configuration Server are dependent on, and must be co-resident with, a Configuration Server. Therefore, by default, they inherit the Configuration Server's operating system-and-level dependencies, as listed in the following table.

The operating systems and levels that are listed in this table are the *minimum requirements*; subsequent patches, fixes, and service packs that have been/are added to these minimum levels are/will be supported as well.

**Table 7: Distributed Configuration Server Operating Systems and Levels**

<b>Platform</b>	<b>Operating System and Level</b>
<b>Windows</b>	NT 4.0 Server, Service Pack 6
	2000 Server, Service Pack 3
	2003 Server, Service Pack 1
	XP Professional, Service Pack 2
<b>UNIX</b>	HP-UX (PA-RISC 1.1 and 2.0), Version 10.20
	Red Hat Enterprise Linux, ES Version 3.0
	SuSE Enterprise Server, Version 9.0
	Solaris, Version 2.7



Although **AIX, Version 4.3** is supported by the HP OpenView Configuration Server Using Radia, support for this platform is currently unavailable for the Distributed Configuration Server.

## Distributed Configuration Server Directories

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

## Source

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

- Windows

`SystemDrive:\Novadigm\IntegrationServer` and its subdirectories

- UNIX

`/opt/Novadigm/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 Distributed Configuration Server execution will add `IntegrationServer_directory\data\dcs`.

## Destination

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

- Windows

`SystemDrive:\ProgramFiles\Novadigm\dcs`

`SystemDrive:\ProgramFiles\Novadigm\dcs\lib`

`SystemDrive:\ProgramFiles\Novadigm\dcs\log`

`SystemDrive:\ProgramFiles\Novadigm\dcs\master*`

`SystemDrive:\ProgramFiles\Novadigm\dcs\slave*`

`SystemDrive:\ProgramFiles\Novadigm\lib`

- UNIX

`/opt/Novadigm/dcs`

`/opt/Novadigm/dcs/lib`

`/opt/Novadigm/dcs/log`

`/opt/Novadigm/dcs/master*`

`/opt/Novadigm/dcs/slave*`

`/opt/Novadigm/lib`

If there is an existing installation of the Distributed Configuration Server, the parameter, IDMASYS, is added to the `nvd.ini` file in the following existing directories.

- Windows  
`SystemDrive:\ProgramFiles\Novadigm\lib`
- UNIX  
`/opt/Novadigm/lib`

## Distributed Configuration Server Space Requirements

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

## Installing the Distributed Configuration Server

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

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

### UNIX Pre-Installation Notes

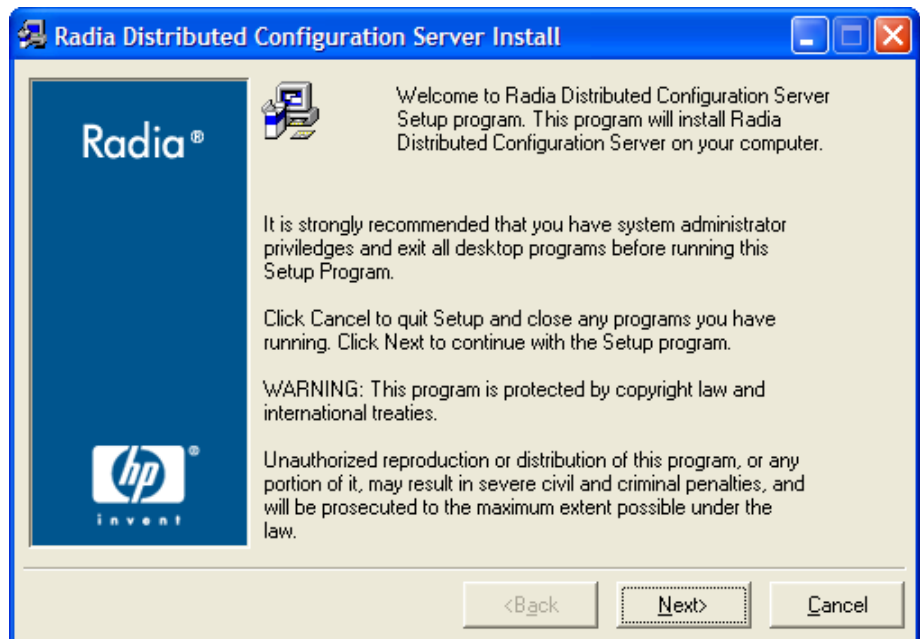
Make sure the user that is performing the installation has:

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

#### To install the Distributed Configuration Server

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

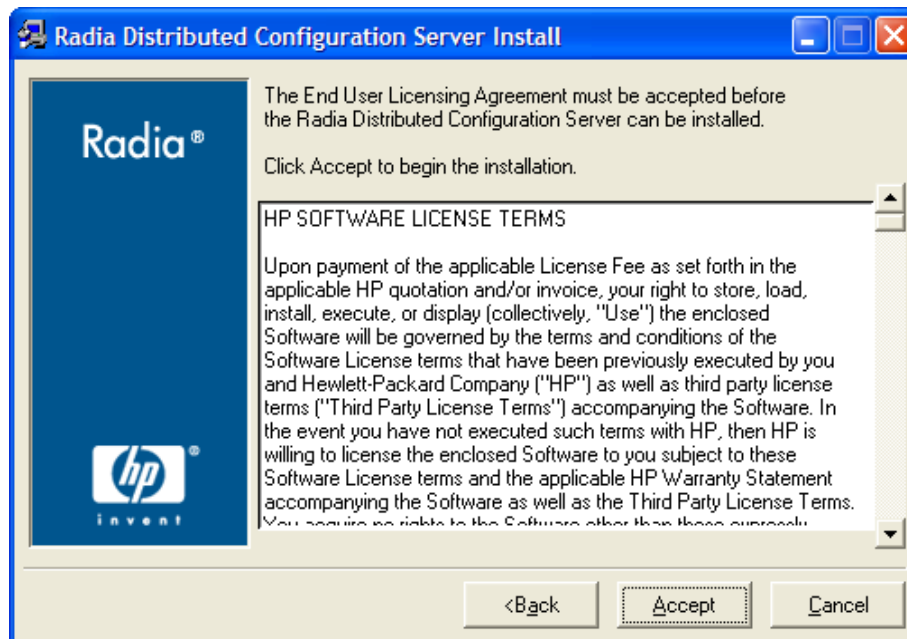
The Distributed Configuration Server Install Welcome window opens.



- 3 Click **Next**.

The Distributed Configuration Server Install HP Software License Agreement window for Distributed Configuration Server opens.



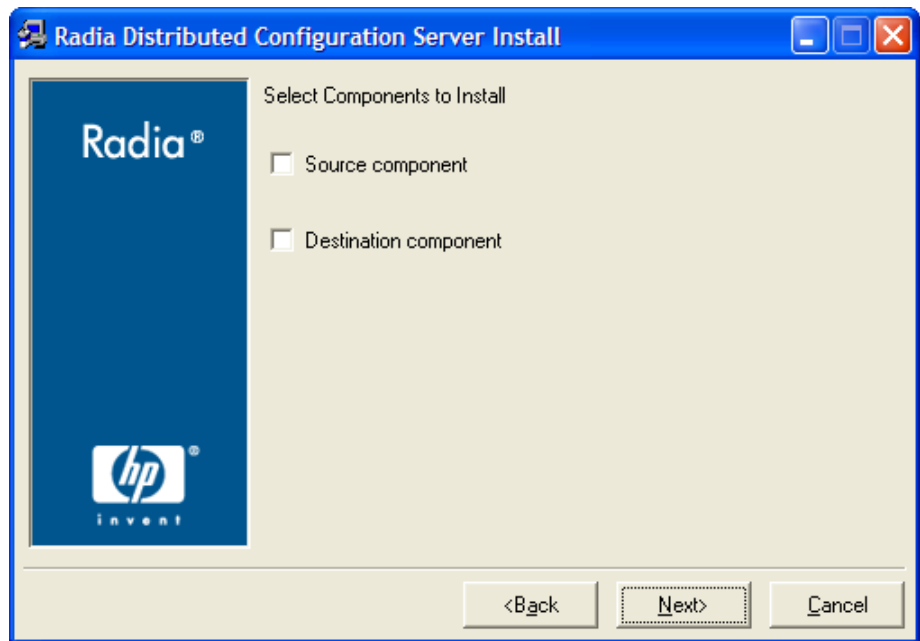


- 4 Click **Accept**.



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

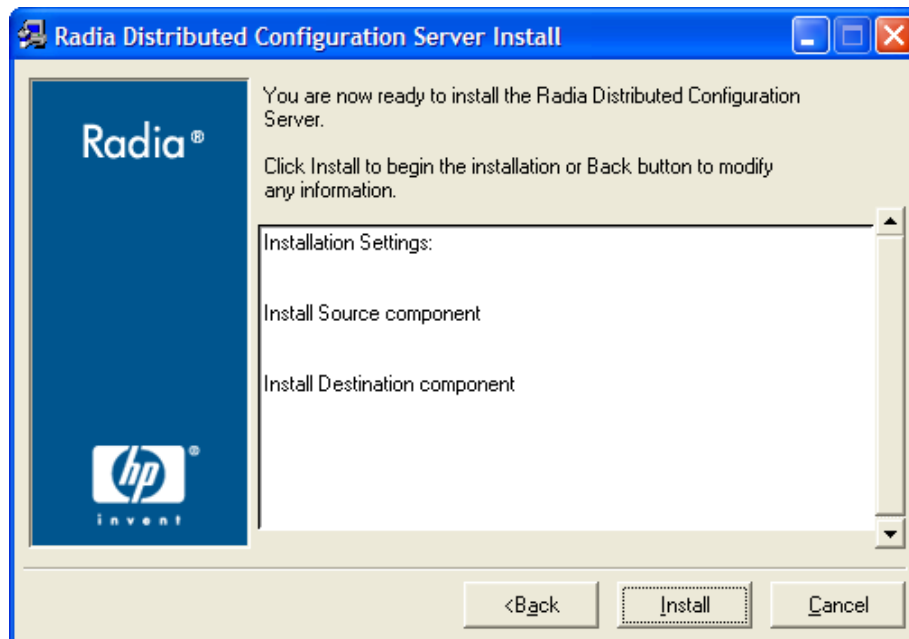
The Distributed Configuration Server Installation Component Selection window opens.



— Select either, or both, of the Distributed Configuration Server components.

5 Click **Next**.

The Distributed Configuration Server Installation Summary window opens.



The Summary window will display which Distributed Configuration Server components will be installed.

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

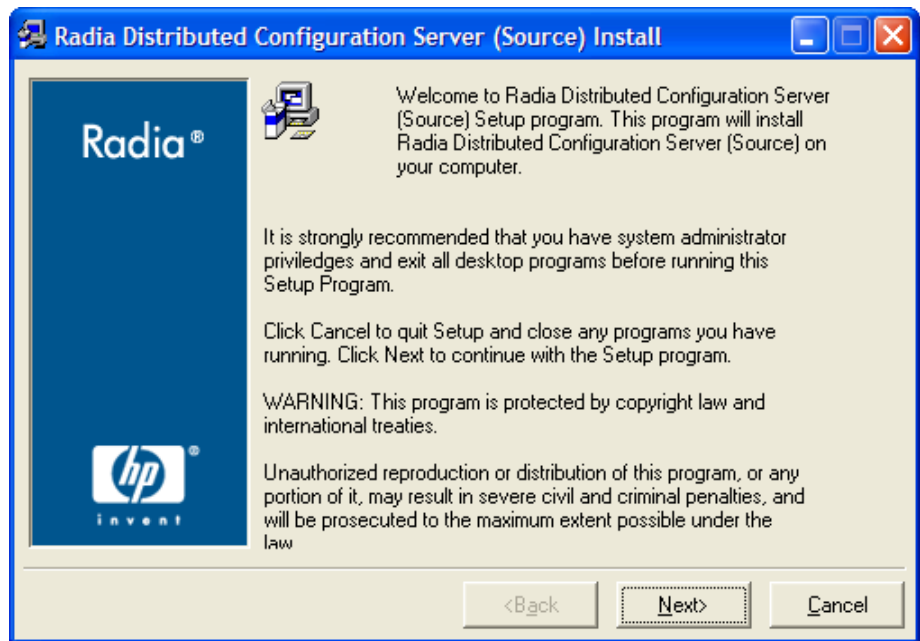
- 6 To install the displayed components, click **Install**.

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

## Installing the Distributed Configuration Server Source Component

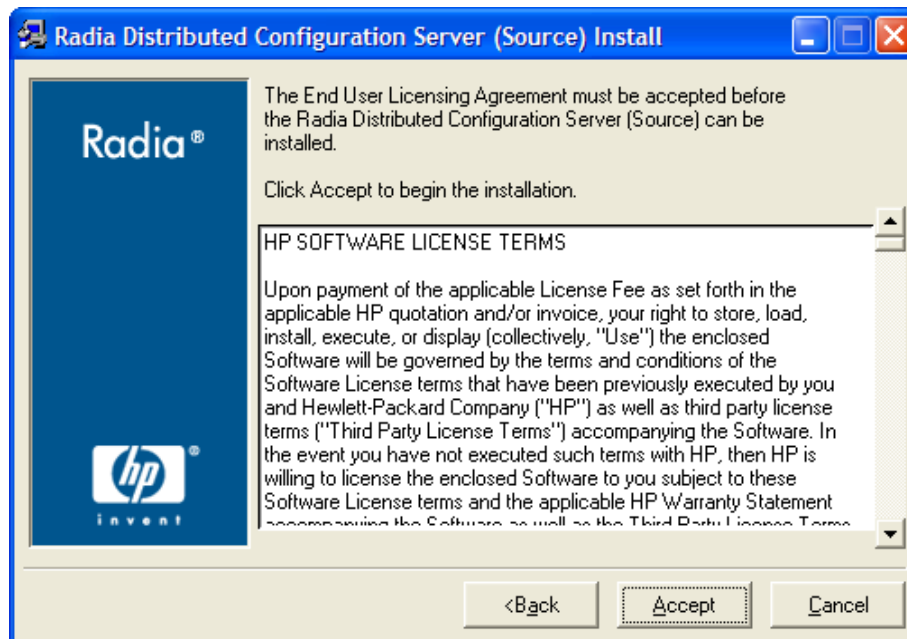
This section describes the installation of the Source component of Distributed Configuration Server.

The Distributed Configuration Server (Source) Install Welcome window appears.



- 1 Click **Next**.

The Distributed Configuration Server (Source) Install HP Software License Agreement window for the Distributed Configuration Server Source component opens.

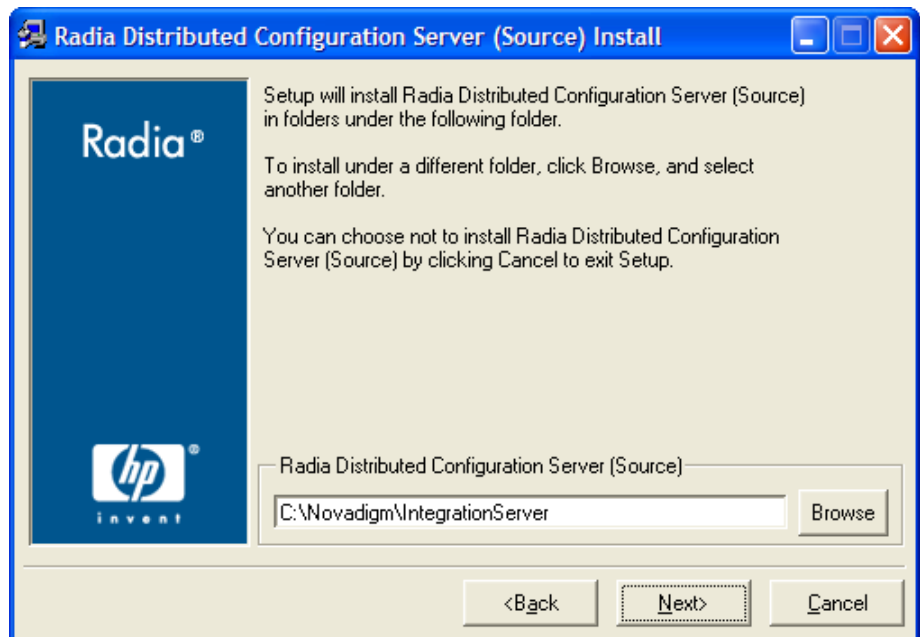


- 2 Click **Accept**.



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

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



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

- If the installation program detects an existing Radia element (such as a Radia client, HP OpenView Administrator Workstation Using Radia, or a previous version of Distributed Configuration Server), the window will have one field—for the installation location.

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

- If the installation program detects no existing Radia 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.

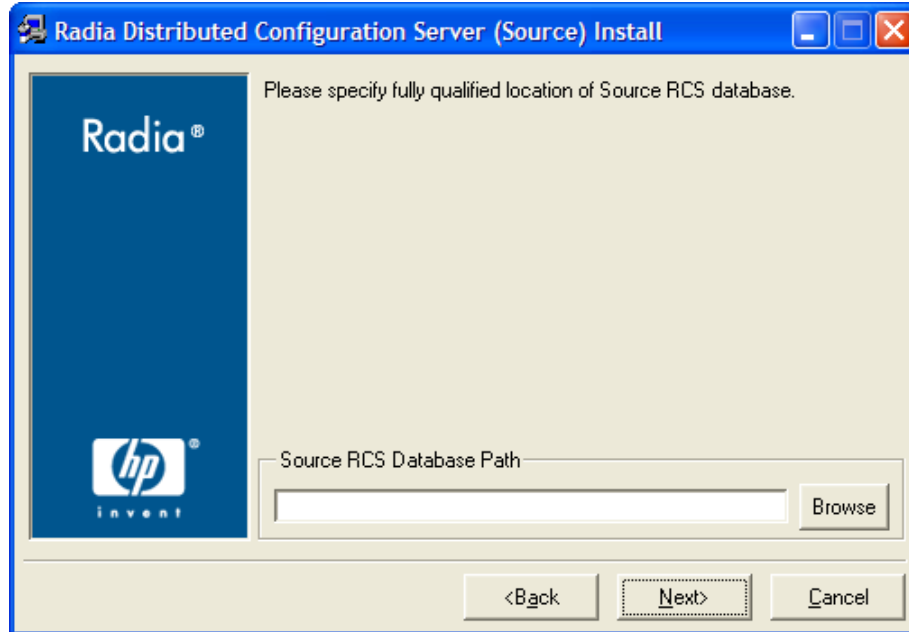
Click **OK** to proceed and allow the update, or click **Cancel** to return to the **Installation Location** window and specify a different directory.

- Accept the default path that is displayed; or

- Specify a different location; or
- Click **Browse** to navigate to a different location.

3 Click **Next**.

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

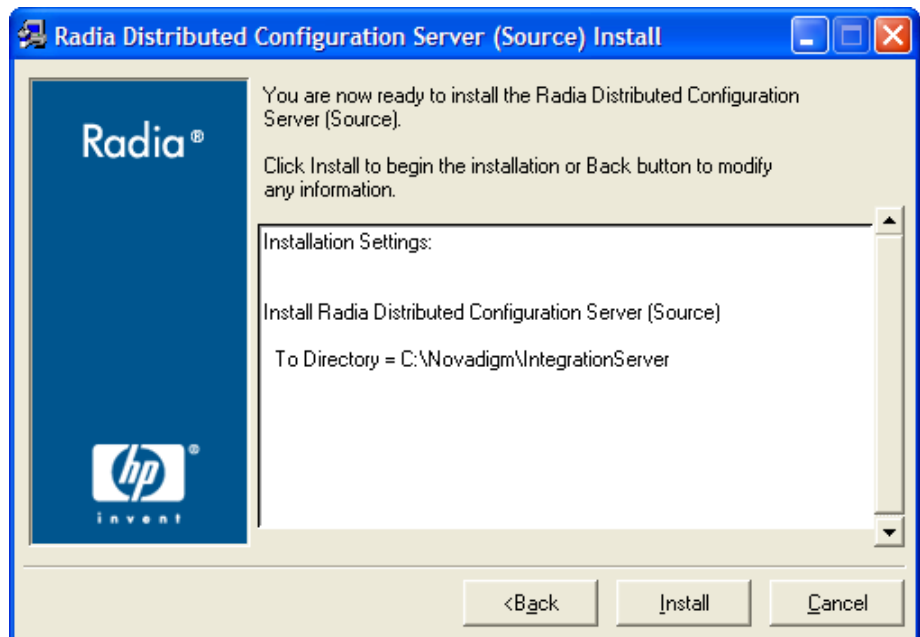


The **RCS Database Path** field displays the directory in which the Radia database was installed.

- Accept the path that is displayed in the window; or
- Specify a different location; or
- Click **Browse** to navigate to a different location.

4 Click **Next**.

The Distributed Configuration Server (Source) Install Summary window opens.



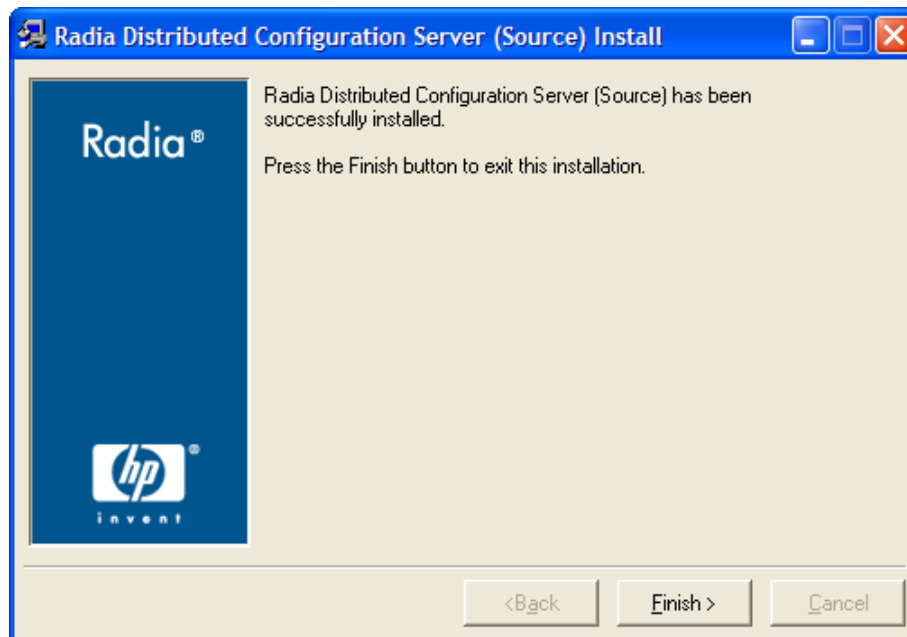
The Summary window displays the directory into which the Distributed Configuration Server Source component will be installed.

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

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

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





6 Click **Finish**.

The Source component of Distributed Configuration Server has installed successfully.

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

## Installing the Distributed Configuration Server Destination Component

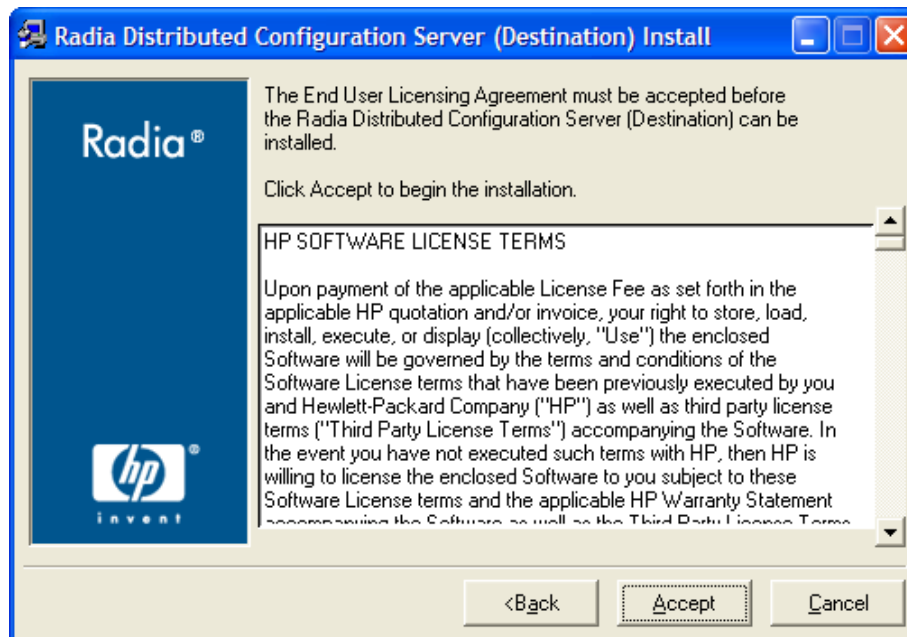
This section describes the installation of the Destination component of Distributed Configuration Server.

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



- 1 Click **Next**.

The Distributed Configuration Server (Destination) Install HP Software License Agreement window for the Distributed Configuration Server Destination component opens.

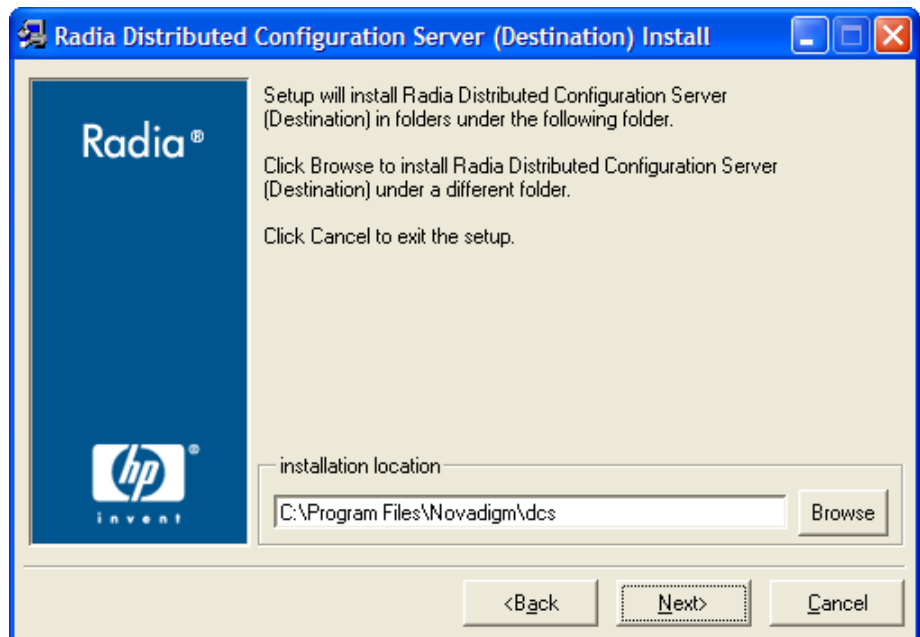


2 Click **Accept**.



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

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



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

- If the installation program detects any existing Radia element (such as a Radia client, HP OpenView Administrator Workstation Using Radia, or a previous version of Distributed Configuration Server), the window will have one text field—for the installation location.

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

- If the installation program detects no existing Radia 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; or
- Specify a different location; or

— Click **Browse** to navigate to a different location.

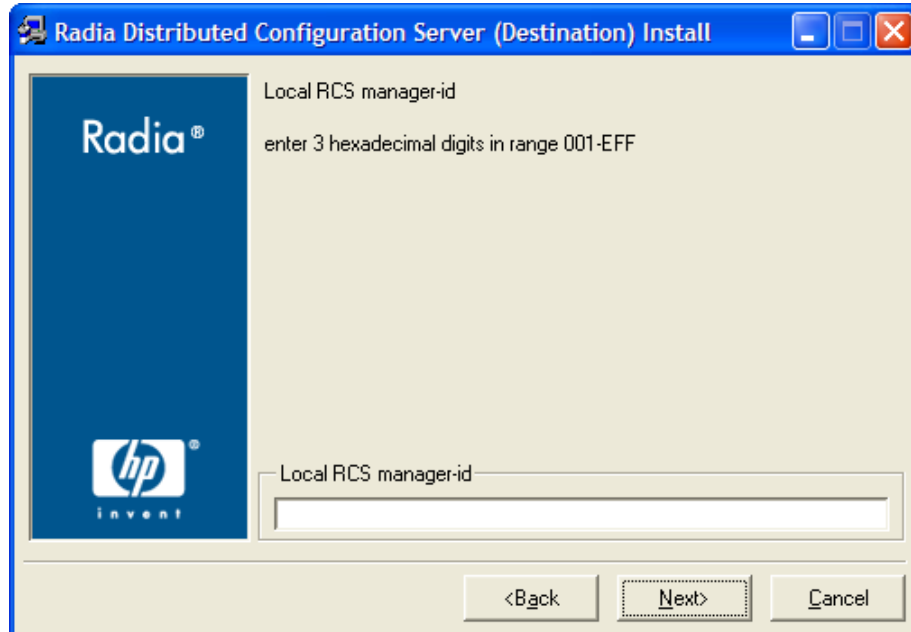
3 Click **Next**.



The next two windows (Local RCS Manager ID and Local RCS Port) will NOT appear if a Configuration Server is installed on this machine; this information will be read in from the Configuration Server's `edmpprof` file.

If there is an existing Configuration Server, continue with step 5 on page 54.

The Distributed Configuration Server (Destination) Install Local RCS Manager ID window opens.



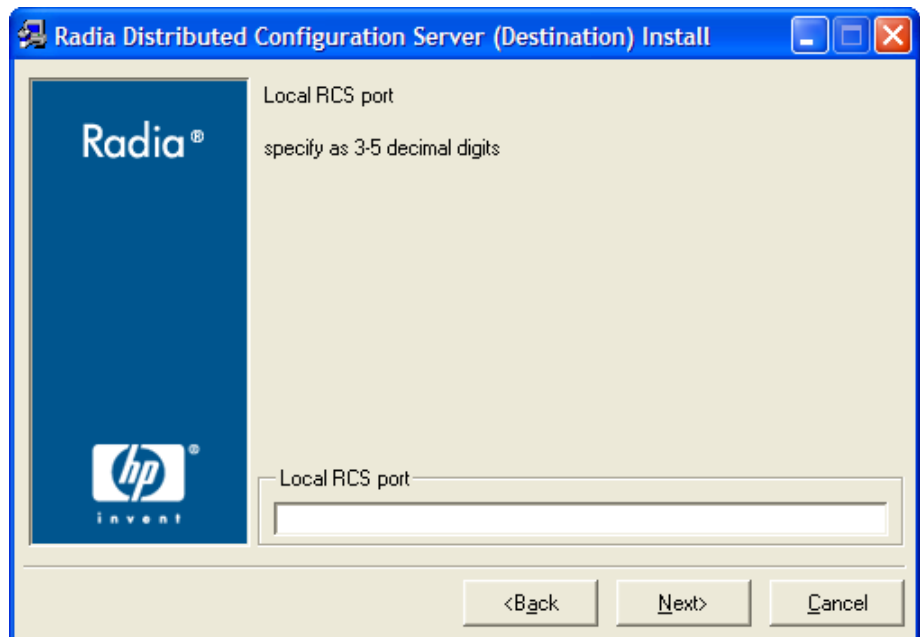
In this window, specify the ID (MGR\_ID) that was assigned during the installation of the Configuration Server that is installed on this machine.

— Specify a valid 3-character, hexadecimal RCS ID.

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

4 Click **Next**.

The Distributed Configuration Server (Destination) Install Local RCS Port window opens.



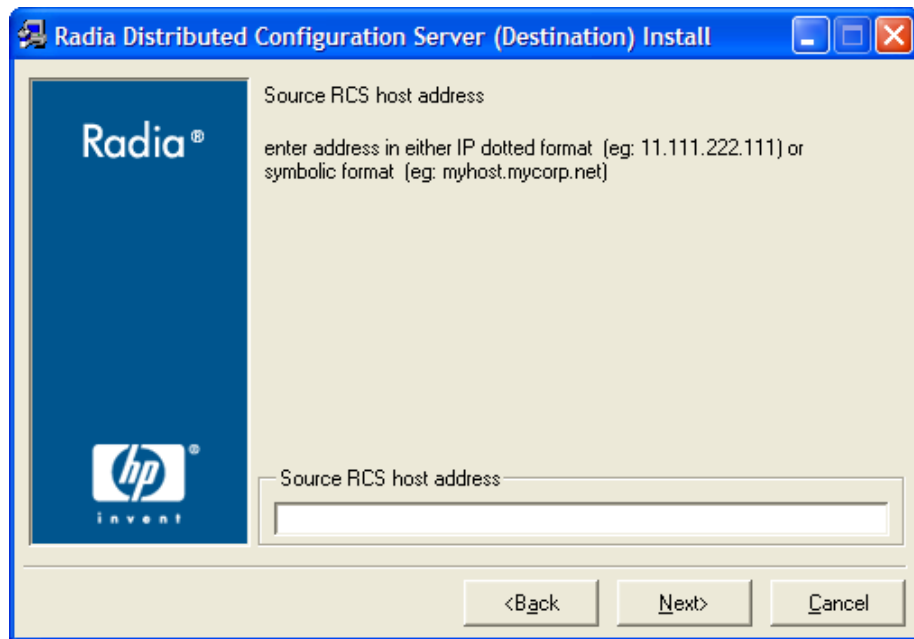
In this window, specify the port of the Configuration Server that is installed on this machine.

— Specify a valid 3- to 5-character decimal RIS port.

5 Click **Next**.

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

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

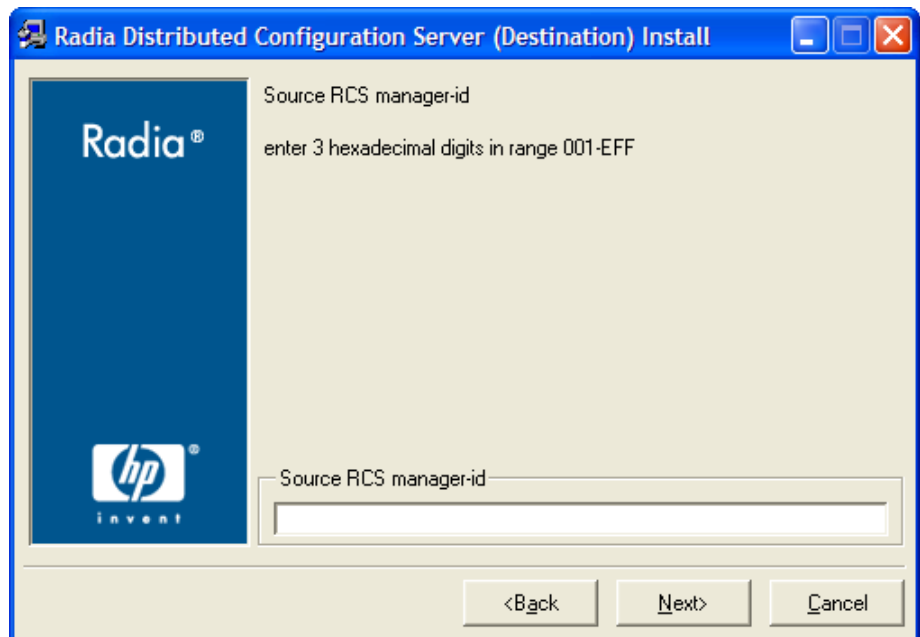


The **Source RCS Host Address** field is where the IP address of the Source Configuration Server is specified.

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

6 Click **Next**.

The Distributed Configuration Server (Destination) Install Source RCS Manager 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 RCS ID.

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

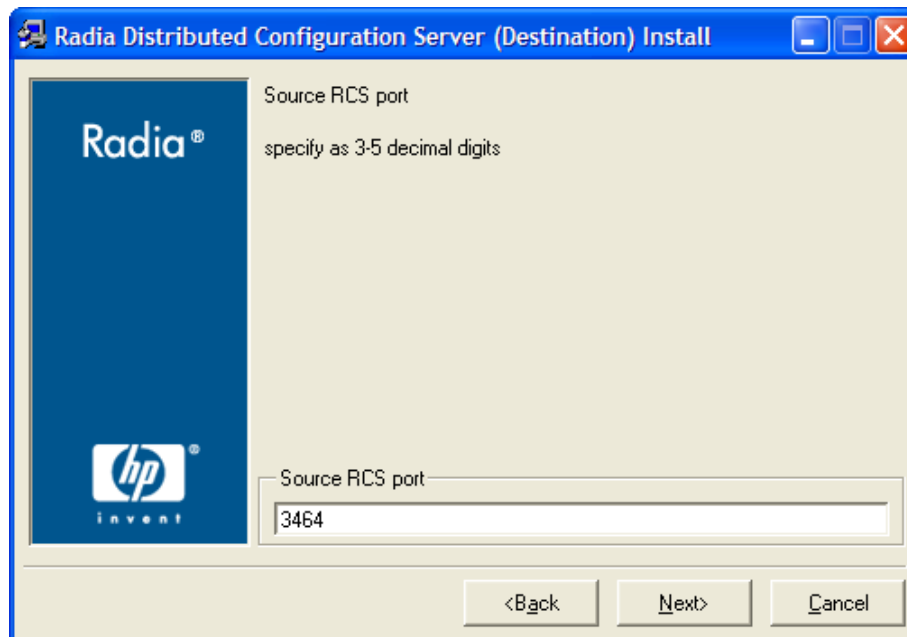
- ▶ The installation will accept any valid 3-character, hexadecimal RCS ID value, as described above.

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 RCS ID verification in the environment.

- 7 Click **Next**.

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





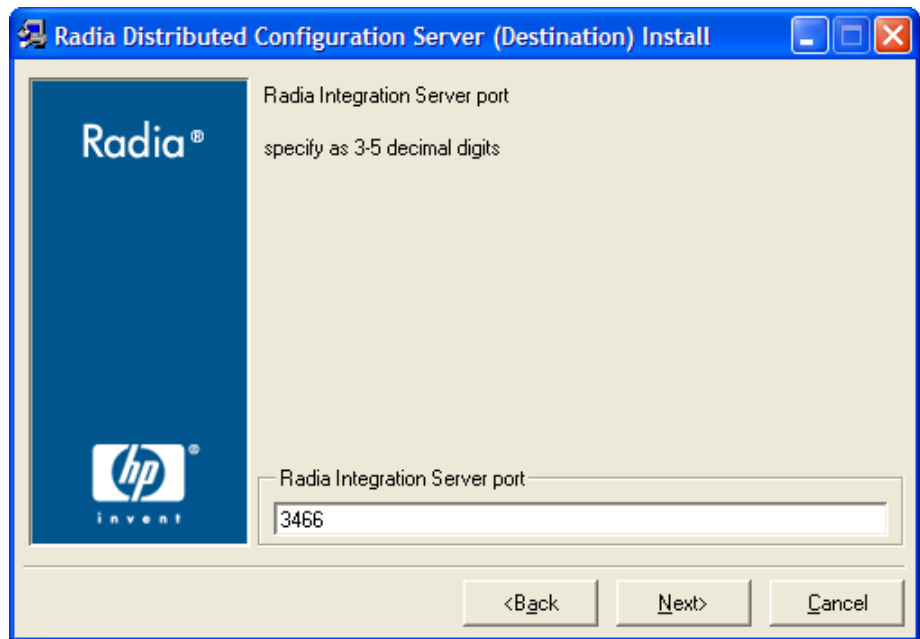
In this window, specify the port of the Source Configuration Server whose ID was specified in the previous window.

► 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.

— Specify a valid 3- to 5-character decimal RIS port.

8 Click **Next**.

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

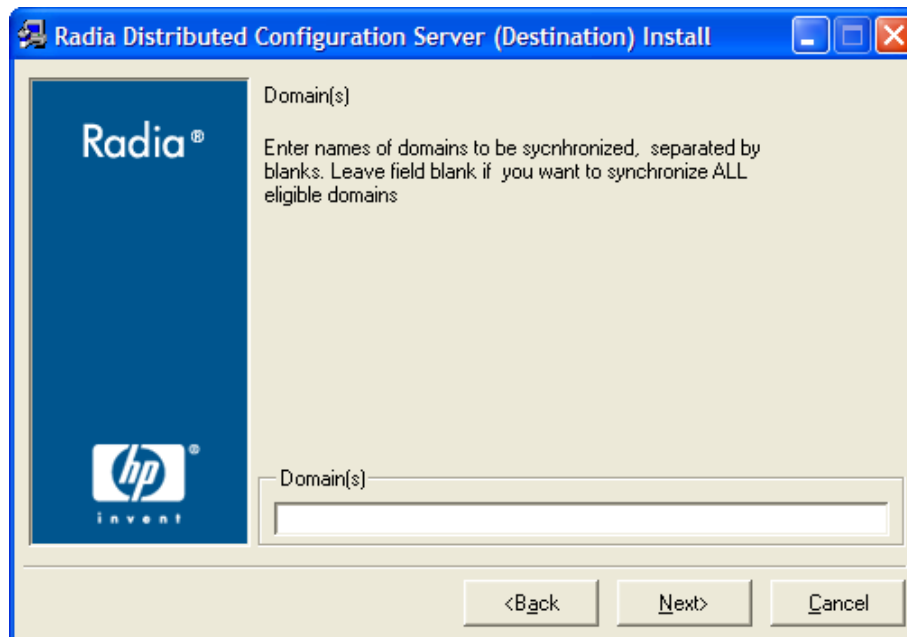


In this window, specify the port of the Integration Server.

— Specify a valid 3- to 5-character decimal RIS port.

9 Click **Next**.

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

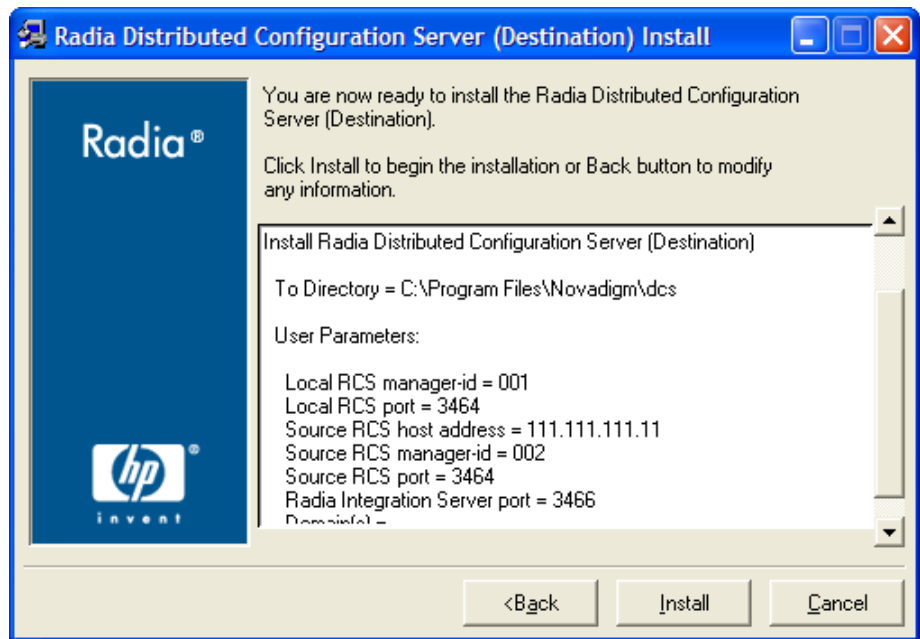


In this window, specify the domains that will be included in synchronizations between this (Destination) RCS and the Source RCS that has been defined in the previous windows.

- To include all eligible domains, leave the **Domains** field blank.
- To include multiple domains, specify the domain names separated by a space.

10 Click **Next**.

The Distributed Configuration Server (Destination) Install Summary window opens.

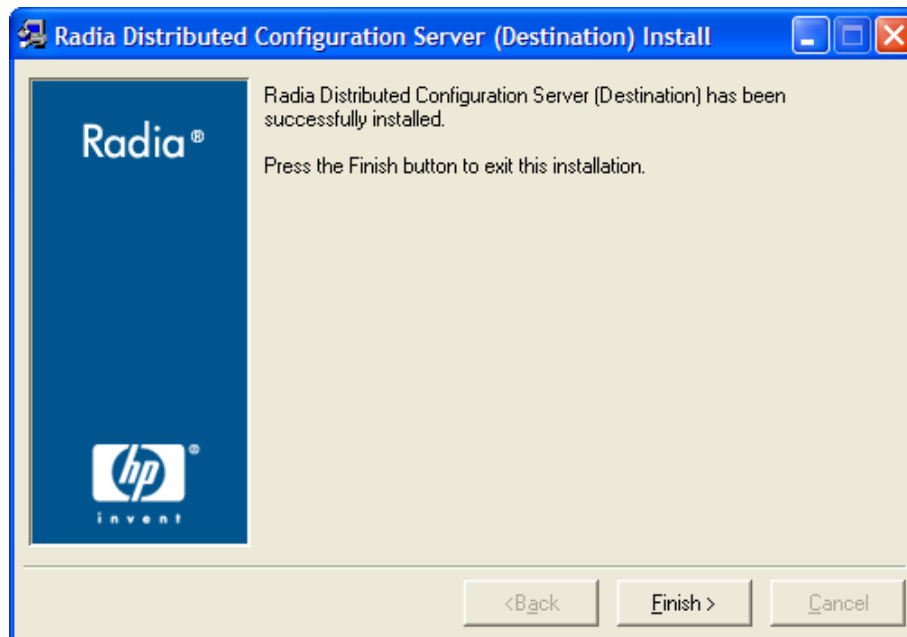


The Summary window displays the directory into which the Distributed Configuration Server Destination component will be installed.

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

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

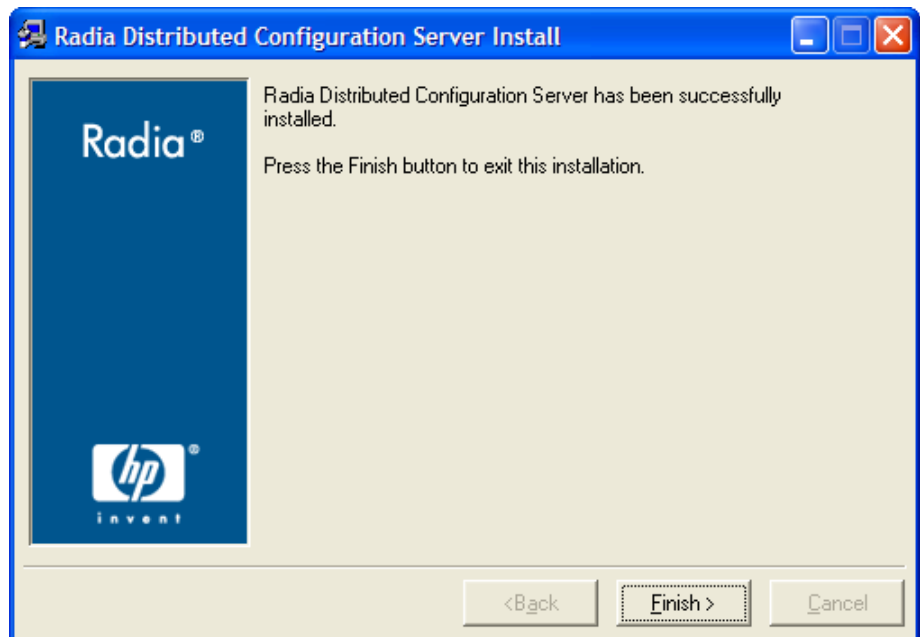
The Distributed Configuration Server (Destination) Install Finish window opens.



12 Click **Finish**.

The Destination component of Distributed Configuration Server has installed successfully.

The Distributed Configuration Server Install Finish window opens.



13 Click **Finish**.

Both components of Distributed Configuration Server have been installed successfully.



**Windows**

- This installation might create a new (or update an existing) `nvd.ini` file in `C:\Program Files\Novadigm\lib`.
- If there was an `nvd.ini` file under `C:\Program Files\Novadigm\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`.

# Setting a Temporary Directory

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

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

## Source Component

By default, the Source component's temporary files are created in a sub-directory 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:/Novadigm/Configuration Server/db
}
```

Save and close the configuration file and re-start the Integration Server.

## Destination Component

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

```
array set 0 {
    -temp-dir c:/rdcs-dest
    -http-host ""
    -http-port 3466
}
```



### All Platforms

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

Save and close the configuration file and re-start the Configuration Server.





---

## 4 Distributed Configuration Server Security

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

- Set up *password protection* for Distributed Configuration Server synchronizations by assigning security control to the host operating system

# 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 Radia 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 Radia databases. Distributed Configuration Server defines only one user ID and password. Therefore, all secured Radia databases that Distributed Configuration Server might access must:

- Be defined in their host's security system,
- Have the user ID in their ADMIN\_LIST, and
- Have the same password for that user ID.



The user ID and password are defined in the Batch Security panel (see page 68) of the Distributed Configuration Server Options.

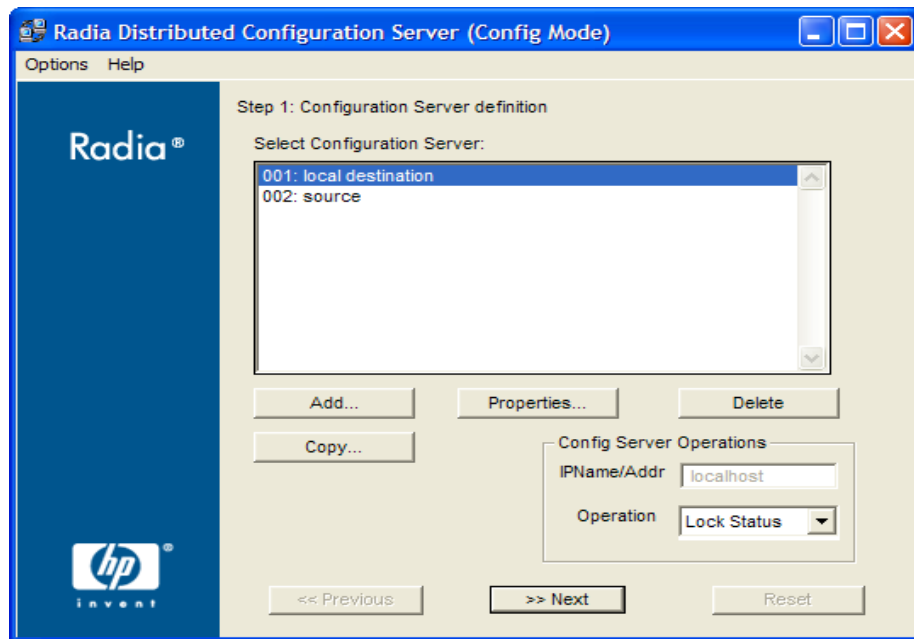
## Enabling Native Operating-System Security

The following sections describe the steps that are required in order to assign password protection-security to the native operating system.

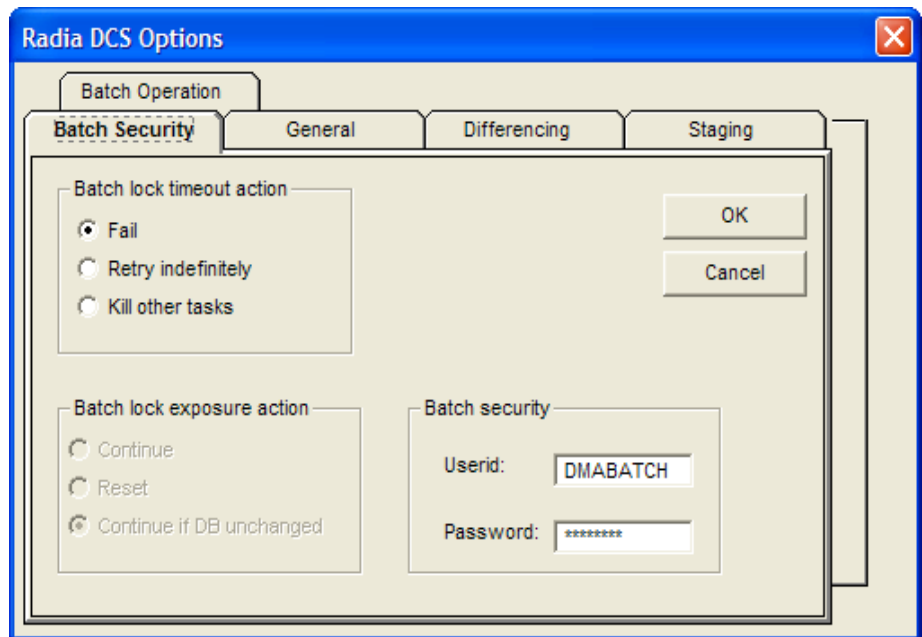
### To set up password protection in Distributed Configuration Server

- 1 On the Destination Configuration Server, open the Distributed Configuration Server (Config Mode) dialog box by clicking **Start, Programs, Distributed Configuration Server (Destination side), and Configure**.

The Distributed Configuration Server (Config Mode) dialog box opens.



- 2 Highlight the Configuration Server that is to be assigned password protection.
- 3 Click **Options**.
- 4 In the drop-down menu that opens, click **Options**.  
The Radia DCS Options panel appears.
- 5 Click the tab, **Batch Security**.  
The Radia DCS Options, Batch Security options panel is displayed.



- 6 In the **Batch Security** area, specify a user ID and Password to be used for password protection.

➤ The default user ID and password are DMABATCH.

- 7 Click **OK**.

You are returned to the Configuration Server definition dialog box.

- 8 Close Distributed Configuration Server.

Password protection has been defined.

## Configuration Server Security Settings

In addition to the steps outlined in the previous section, 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 at Configuration Server installation because it is not needed for default operations.  
It can be added to the `edmprof` file in order to configure Distributed Configuration Server as a default function of the Configuration Server.

To modify the `edmprof` file

- 1 Bring down the Configuration Server.
- 2 Open the `edmprof` file using a text editor.
- 3 Add the section, MGR\_DMA, and the settings shown below:  

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

 For a description of these settings, see Table 8.
- 4 Save the changes, 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 example, **Act as part of the operating system** on Windows NT).  
For information on establishing operating system-specific user rights and policies, consult the operating system’s product documentation.

Table 8 presents a description of the two MGR\_DMA settings that are required in order to establish native operating-system security.

- ▶ An additional, optional MGR\_DMA setting, DMA\_TIMEOUT, is detailed in Table 11 on page 86.

**Table 8: MGR\_DMA Settings and Values**

Setting	Explanation of Value
SECURITY_METHOD	Optional. If not specified, security verification is disabled. To enable native operating-system security, specify <b>EDMSIGN</b> .

<b>Setting</b>	<b>Explanation of Value</b>
ADMIN_LIST	This setting is required if a SECURITY_METHOD is specified. Specify the list of administrators (user IDs) that are allowed to use Distributed Configuration Server on this Radia database. The format is a comma-separated (no spaces), case-sensitive list of operating-system account names.

---

# 5 Setting Up a Distributed Configuration Server Synchronization

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

- Define (add, copy, and delete) Configuration Servers in Distributed Configuration Server
- Specify the properties of the Configuration Servers that are defined in Distributed Configuration Server
- Set up a Distributed Configuration Server operation by choosing a synchronization pair and eligible domains

# Configuration Servers in Distributed Configuration Server

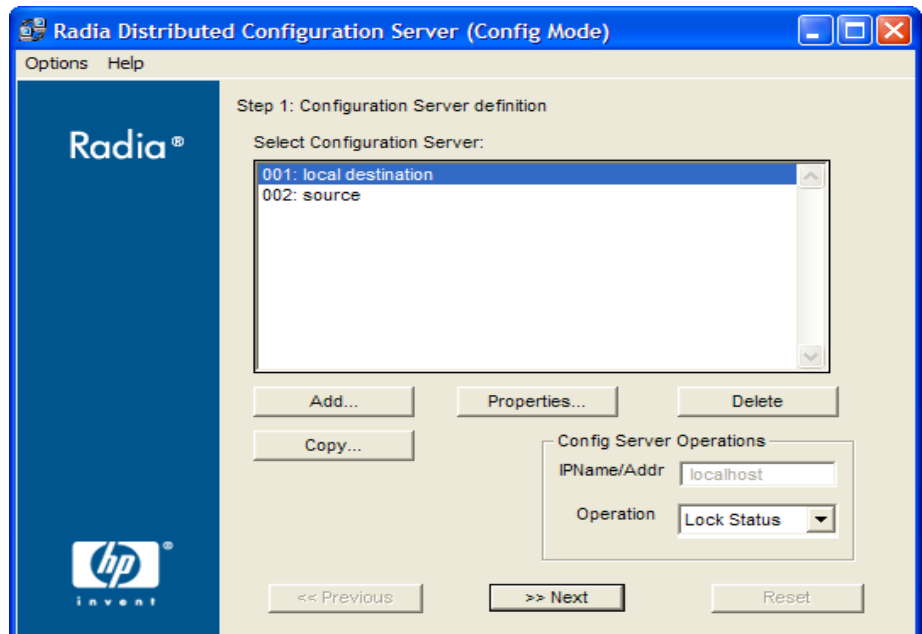
This section describes how, in Distributed Configuration Server, to add, copy, and delete Configuration Servers.

## Adding Configuration Servers

To add Configuration Servers in Distributed Configuration Server

- 1 On the Destination Configuration Server, open the Distributed Configuration Server (Config Mode) dialog box by clicking **Start, Programs, Distributed Configuration Server (Destination side), and Configure.**

The Configuration Server definition dialog box appears.



- If a previous version of Distributed Configuration Server/EDM DMA exists, the previously defined Configuration Servers will appear.



- 2 Click **Add**.

The Configuration Server Properties dialog box appears.

Configuration Server Properties

ID (3 chars): 001

Description: local destination

Protocol: TCP

Timeout (secs) 3600

Streaming

Compression

This id shared

TCP/TCPs

Verify Name/Add

Name/Addr: localhost

Port: 3464

Proxy Server

Name/Addr:

Port: 8080

Userid:

Password:


OK Cancel

- 3 Specify the appropriate Configuration Server information, as shown in the following table.

**Table 9: Configuration Server Properties**

<b>Field</b>	<b>Description</b>	<b>ZMANAGER Variable</b>
ID (3 chars.)	Using the characters 0-9 and A-F specify the three-character, hexadecimal ID for the Configuration Server. This must match the value of MGR_SETUP.MGR_ID for the selected Configuration Server.  Exception: The 256 consecutive positions from F00 through FFF are reserved for use with HP OpenView Using Radia.	ZMGRID
Description	Specify an alphanumeric (255 characters maximum) Configuration Server description that will readily identify this Configuration Server. For example, <b>Server_East_001</b> .  Note: This description is independent of the Configuration Server name that was assigned at installation, but can be the same.	ZMGRNAME
Protocol	This field is disabled. The only supported protocol is TCP/IP.	ZCOMTYPE
Timeout	Specify a timeout (in seconds) for how long Distributed Configuration Server is to wait to complete a task.  Note: If Distributed Configuration Server times out before the tasks end, it will abort.	ZTIMEO
Streaming	This option is disabled. The only value for streaming is ON.	N/A
Compression	This option is disabled. The only value for compression is ON.	N/A
This ID shared	Select this check box to enable the IPName/Addr field in the <b>Config Server Operations</b> area of the Configuration Server definition panel.  Note: This must be selected in order to support Cloned Managers (see Table 4, on page 18).	N/A
TCP/TCPS		
Verify Name/Addr	Check this option in order to have Distributed Configuration Server verify that the host name or IP address that is specified for Name/Addr is known in the host's table. (Optional)	N/A


Field	Description	ZMANAGER Variable
Name/Addr	Specify the IP name, IP address, or URL of the host Configuration Server. (Required)	ZTCPADDR
Port	Specify the IP port of the host Configuration Server. (Required)	ZTCPPOINT
Proxy Server	This option is disabled.	N/A

- 4 After specifying the properties for the Configuration Server, click **OK**.  
A Configuration Server has been added to Distributed Configuration Server.
  -  To define additional Configuration Servers to Distributed Configuration Server, repeat steps 2 and 3, or use the Copy option that is described in the next section, Copying Configuration Servers.

## Copying Configuration Servers

In addition to adding Configuration Servers to Distributed Configuration Server, they can be defined by copying the definition of an existing one, and then modifying it.

### To copy Configuration Servers in Distributed Configuration Server

- 1 On the Destination Configuration Server, open the Distributed Configuration Server (Config Mode) dialog box.
- 2 Select the Configuration Server that is to be duplicated, and click **Copy**.  
The Configuration Server Properties dialog box appears.  
The ID field will be blank.
- 3 Type a unique, 3-character, hexadecimal ID.
  -  Only a unique ID will be accepted; if a duplicate ID is specified, an error message will appear.
- 4 Modify any of the other fields as needed. (For assistance, see Table 9 on page 74.)

- 5 Click **OK**.

A Configuration Server has been copied within Distributed Configuration Server.

## Deleting Configuration Servers

To delete Configuration Servers from Distributed Configuration Server

- 1 With the Configuration Server definition dialog box open, highlight the Configuration Server that is to be deleted.

- 2 Click **Delete**.

A confirmation message will appear to verify that the specified MGR\_ID should be deleted.

- 3 If the wrong Configuration Server was selected, click **Cancel** and select the correct Configuration Server.

To delete the Configuration Server specified, click **Delete**.

The Configuration Server will be removed from the **Select Configuration Server** list on the Configuration Server definition dialog box.

- 4 Close Distributed Configuration Server.

A Configuration Server has been deleted from the Distributed Configuration Server agent.

## List of Configuration Servers

Each time the Configuration Server definition dialog box is accessed, Distributed Configuration Server will display the list of Configuration Servers that are defined to it.

# Distributed Configuration Server Configuration

The configuration-only interface allows an administrator to set up the parameters of the synchronization, which must then be run in the batch mode. The interface is comprised of two panels, as described in the sections, Configuration Server Definition Panel (starting on page 78) and Choose Configuration Servers and Domains Panel (starting on page 80).

## Navigation Buttons and Menu Options

Both of the Distributed Configuration Server configuration dialog boxes have navigation buttons in the lower part of the window, and two menu options (**Options** and **Help**) in the upper left corner.

### Navigation Buttons

The navigation buttons (**Previous**, **Next**, and **Finish**) allow for movement between the panels.

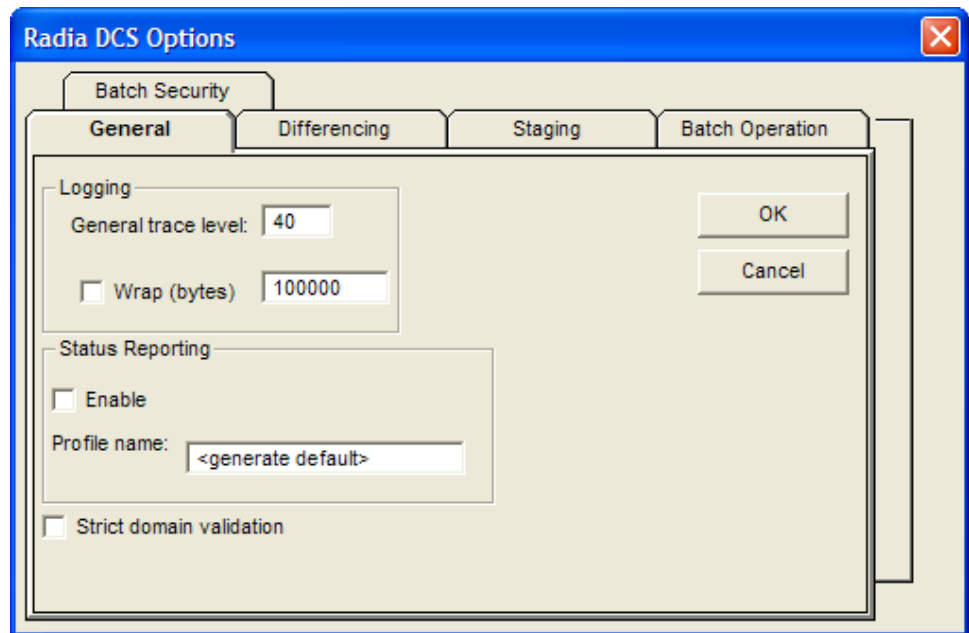


To stop Distributed Configuration Server without completing the configuration, click the standard **Close** button (**X**) on the title bar.

### Menu Options

In the upper left corner of the Distributed Configuration Server windows, there are two menu options (**Options** and **Help**).

- **Help** offers one option, **About**, which presents Distributed Configuration Server version information.
- **Options** offers one option, **Options**, which presents the five-tab Radia DCS Options panel.



**Figure 1: The five-tab Distributed Configuration Server Options panel.**

The Distributed Configuration Server configuration options are discussed in detail in Chapter 6, *Configuring Distributed Configuration Server Options*.

## Configuration Mode Panels

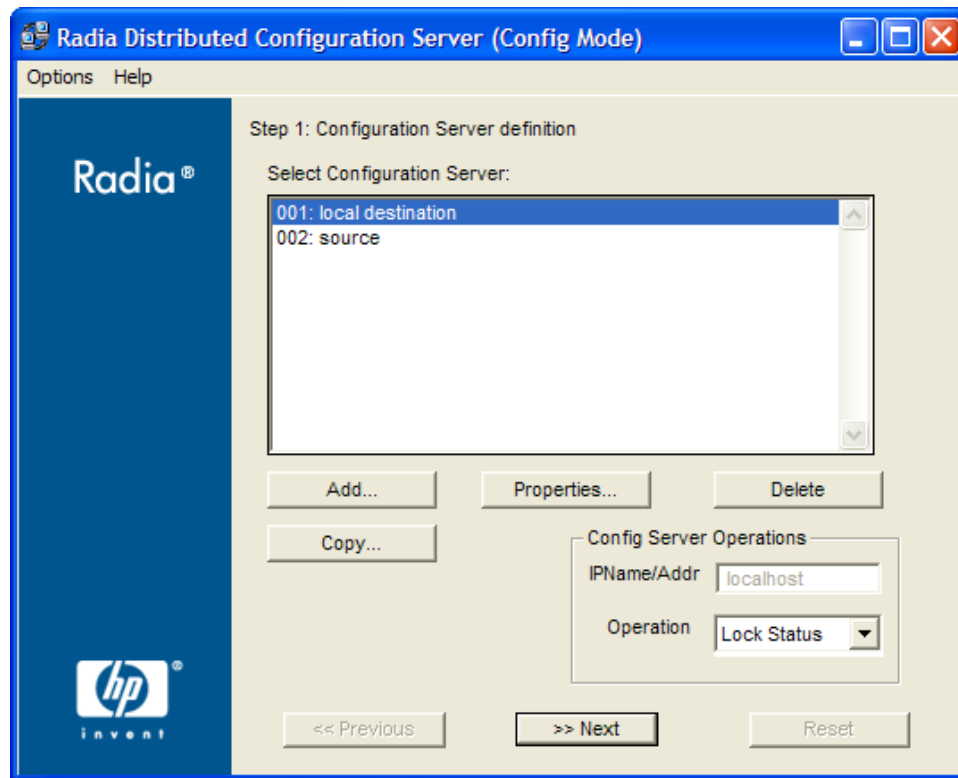
The **Config Mode** provides a two-panel interface that takes an administrator through the configuration of the Distributed Configuration Server synchronization process. The two panels are:

- Configuration Server Definition Panel (see the section below)
- Choose Configuration Servers and Domains Panel (see page 80)

### Configuration Server Definition Panel

In the first panel, Configuration Servers are defined (added, copied, and deleted), as described in the section, *Configuration Servers in Distributed Configuration Server*, starting on page 72; and their lock-status operations

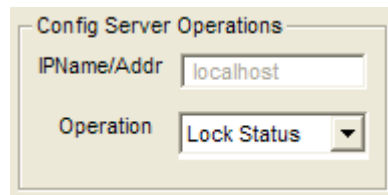
can be queried, as described in the section, Operation: Lock Status, starting on page 80.



**Figure 2: The Configuration Server definition panel after a Configuration Server has been added.**

### Configuration Server Operations

In the Config Server Operations area, a Configuration Server's lock-status can be queried and its IP address overridden.



**Figure 3: The Config Server Operations area.**

## IPName/Addr

In this field, an administrator can specify an override for the selected Configuration Server's IP name/address. The default is the IP name/address that is configured in ZMANAGER.

This field is disabled and displays the IP address of the Configuration Server that is highlighted in the **Select Configuration Server** field. The field will become enabled if, on the Configuration Server Properties panel, the option **This id shared**, has been selected for that Configuration Server.



This supports Configuration Server operations on Cloned Managers (see Table 4 on page 18).

## Operation: Lock Status

This lets an administrator query the lock status of a Configuration Server.

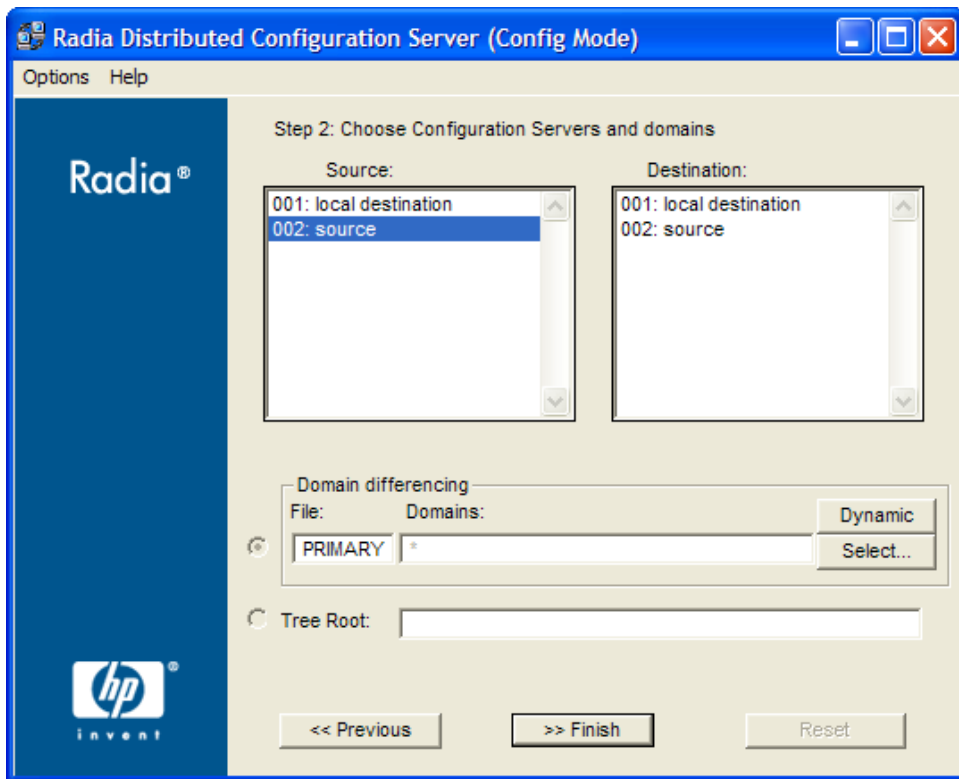
- 1 Highlight a Configuration Server in the **Select Configuration Server** field.
- 2 Click the down arrow next to **Lock Status**.
- 3 Click **Lock Status**.

Shortly, a message will pop up, reporting the database lock-status of the selected Configuration Server.

## Choose Configuration Servers and Domains Panel

In the second panel, an administrator selects the synchronization pair and the Radia database domains that are to be included in the synchronization, as described in the section, Choosing Configuration Servers and Domains, starting on page 82.





**Figure 4: The Choose Configuration Servers and domains panel.**

➤ In this window, the buttons **Previous** and **Finish** are activated.

With these two steps completed, the Distributed Configuration Server synchronization is ready to be run in the batch mode, which is detailed in Chapter 7, Distributed Configuration Server's DMABATCH.

# Choosing Configuration Servers and Domains

The two Configuration Servers that will participate in a Distributed Configuration Server session are the synchronization pair. Once the synchronization pair is selected the list of eligible domains is generated based on the Configuration Servers and their database control information, such as last synchronization and updates from other Radia components.

To set up a synchronization pair

- 1 Open the Distributed Configuration Server (Destination Component) Config Mode panel.

- 2 Click **Next**.

The Choose Configuration Servers and domains panel appears.

The list of eligible Configuration Servers that have been defined to Distributed Configuration Server will be listed in the **Source** and **Destination** fields of this panel.

- 3 Select one Source and one Destination Configuration Server.



The screenshot shows a configuration window titled "Domain differencing". It has two main sections. The top section has a "File:" label followed by a text box containing "PRIMARY", and a "Domains:" label followed by a text box containing an asterisk (\*). To the right of these text boxes are two buttons: "Dynamic" and "Select...". The bottom section has a "Tree Root:" label followed by an empty text box.

- 4 In the **Domain differencing** area, click either:

- **Select** – to manually specify which domains are to be synchronized. (Continue with step 5.)

or...

- **Dynamic** – to allow Distributed Configuration Server to automatically synchronize all of the eligible domains. (Click **Finish**, the synchronization is configured and ready to be run.)

- ▶ If **Dynamic** is selected, a list of all eligible domains will be automatically generated at run-time. (All domain-eligibility rules still apply.) If new domains are created after the configuration and before the synchronization, they are automatically included in the synchronization.  
If **Dynamic** is selected, an asterisk (\*) will be displayed in the **Domains** field.

With both domain-selection options, a list of eligible domains is built, based on the two Configuration Servers that have been chosen.

- ▶ If there are no eligible domains, a message will appear. If this message appears unexpectedly, the ownership assigned for the expected domains might be incorrect at either of the Configuration Servers. Shut down Distributed Configuration Server and the associated Configuration Servers, and correct the domain ownership using the ZEDMAMS utility, UPDATE\_MGRIDS. After correcting the domain ownership, restart the Configuration Servers and resume Distributed Configuration Server.

If **Select** was chosen, when the eligible-domains list is complete, the Domain Selection dialog box appears.

The eligible domains are listed alphabetically, with their owning MGR\_ID.

- 5 Select one or more of the eligible domains.
- 6 Click **OK**.

The domains that were selected for synchronization are now displayed in the **Domains** field of the Choose Configuration Servers and domains panel.

- 7 Click **Finish** to exit the configuration of this Distributed Configuration Server synchronization.

- ▶ If either Configuration Server requires password setup that has not been assigned, a message will appear indicating that Radia DMABATCH cannot be run.

A Distributed Configuration Server synchronization has been configured.

## The Configuration Server's EDMPROF File

The `edmpprof` file is the text file where the Configuration Server's operational parameters are configured and stored. Two of its sections (MGR\_STARTUP and MGR\_DMA) are integral to enabling Distributed Configuration Server and ensuring its proper operation.

Information on these `edmpprof` sections, including their settings, acceptable values, and impact on Distributed Configuration Server processing is presented in this section.



For a comprehensive look at the `edmpprof` file, refer to the *User Guide for the HP OpenView Configuration Server Using Radia (Configuration Server Guide)*.

### MGR\_STARTUP Section

The MGR\_STARTUP section dictates startup behavior for the Configuration Server. The following MGR\_STARTUP settings are essential to the operation of the Distributed Configuration Server.

**Table 10: MGR\_STARTUP Settings and Values**

Setting	Designated Value	Explanation
MANAGER_TYPE	DISTRIBUTED	This is the default value that is established when the Configuration Server is installed. Note: To ensure that a Configuration Server is Distributed Configuration Server-enabled, do not change this value.
MGR_NAME	32 alphanumeric characters (max.)	This is a Configuration Server identifier. Note: This value is independent of the Configuration Server names that are listed in the Select Configuration Server area of the Configuration Server definition window.

Setting	Designated Value	Explanation
MGR_ID	Unique, 3-digit, hexadecimal ID	<p>A Configuration Server's unique identifier. This must match the ID that is specified in the <b>ID</b> field of the Configuration Server Properties dialog box.</p> <ul style="list-style-type: none"> <li>• Distributed Configuration Server uses this value to generate object IDs in the Radia database.</li> <li>• Each character in this identifier can have the values 0-9 and A-F.</li> </ul> <p>Exception: The 256 consecutive positions from F00 through FFF are reserved for use with HP OpenView Using Radia.</p>
TCP_PORT	Port number on which the Configuration Server will listen.	Must match the Distributed Configuration Server-specified port

### MGR\_ID

The MGR\_ID setting is used to establish a unique identity for each Configuration Server. Distributed Configuration Server uses the MGR\_ID to determine each domain's owning Configuration Server. (All domains have an owning Configuration Server.) 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 Server machines. If they are not, 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 Peer Synchronization, in Table 4 on page 18.

### MGR\_DMA Section

In addition to the MGR\_DMA settings that are needed to establish Distributed Configuration Server password protection (described in the section, Configuration Server Security Settings on page 68), there is another Distributed Configuration Server-related setting, DMA\_TIMEOUT, which is detailed in Table 8.

**Table 11: DMA\_TIMEOUT**

<b>Setting</b>	<b>Explanation of Value</b>
DMA_TIMEOUT	<p>Specify the number of seconds that Distributed Configuration Server is to wait for non-Distributed Configuration Server tasks to complete before applying a lock to the Radia database. If Distributed Configuration Server times out before the task ends, it will abort. The default is 0.</p> <ul style="list-style-type: none"><li>• When soft-locking the Radia database, Distributed Configuration Server must wait for all administrator tasks to end.</li><li>• When hard-locking the Radia database, Distributed Configuration Server waits for all non-Distributed Configuration Server tasks to end.</li></ul> <p>Note: If Distributed Configuration Server is unable to lock either of the databases, it will query the value of Batch Lock Timeout (see Table 19 on page 98).</p>

---

## 6 Configuring Distributed Configuration Server Options

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

- Use the five Radia DCS Options tabs to specify actions to be taken by Distributed Configuration Server during the database synchronization

# Distributed Configuration Server Options

Distributed Configuration Server has a configuration area, Radia DCS Options, which has five tabs that enable an administrator of HP OpenView Using Radia to specify a variety of processing actions, ranging from report generation to database-lock timeout actions. The Distributed Configuration Server Options are comprised of the following tabs:

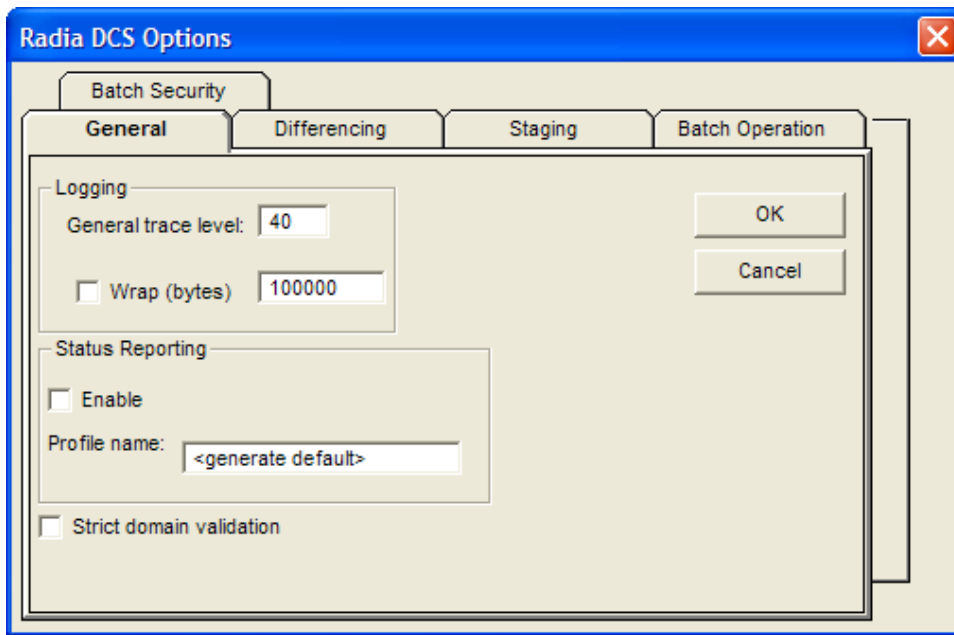
- General Options, below  
logging and status-reporting options
- Differencing Options, on page 94  
options to generate a differencing report and to skip database resources
- Staging Options, on page 95  
option to skip missing resources
- Batch Operation Options, on page 96  
synchronization verifying and session failure options
- Batch Security Options, on page 97  
options for password protection and database-lock timeouts

The following sections describe these options.

## General Options

The **General** options allow an administrator to configure: logging options, status reporting, and domain validation.





**Figure 5: Distributed Configuration Server Options: General options.**


Table 12 describes the options available in this panel.

**Table 12: General Options**

<b>Option (Object Variable)</b>	<b>Settings (defaults in bold)</b>	<b>Description</b>
Logging		
General Trace Level (ZTRACEL)	0 – 999 ( <b>30</b> )	The level of detail for tracing.
Wrap (LOGWRAP)	<b>0=disable</b> 1=enable	Select to enable (1) log wrapping.
Number of Bytes (LOGSIZE)	<b>100,000</b>	Number of bytes at which log text will wrap.

<b>Option (Object Variable)</b>	<b>Settings (defaults in bold)</b>	<b>Description</b>
Status Reporting		<p>This allows Distributed Configuration Server to send, at several processing points, a DMASTATS object (see Table 13 on page 91) to the Source Configuration Server. This object contains data about the state and configuration of Distributed Configuration Server.</p> <p>Note: To save these objects for future reference, use the System Explorer to configure the Source Configuration Server to put them in the PROFILE file of the database, using the PUTPROF command, as described in the section, Using PUTPROF on page 91.</p>
Enable (REPORT)	<b>0=disable</b> 1=enable	The status-reporting facility is enabled by selecting the <b>Enable</b> check box.
Profile Name (REPTNAME)	<generate default>	See the section, ZUSERID starting on page 93.
Strict Domain Validation (STRICT)		<p>When local database updates occur and neither Configuration Server owns the domain, two peer validation rules govern how the updates are handled. By default, this option is disabled.</p> <ul style="list-style-type: none"> <li>• The domain must not be locally updated on the Source after it was last synchronized from the owner. This would propagate updates that are not present at the owner.</li> <li>• The Destination domain must not have been synchronized from a Source domain version that has been updated more recently than that of the owner. Doing so would regress the version at the Destination.</li> </ul> <p>Note: With the current Radia database, these rules cannot be enforced if the Configuration Servers are not all in the same time zone, or if their clocks are not reasonably close. These rules are now enforced optionally, by selecting <b>Strict domain validation</b>.</p>

## Using PUTPROF

- 1 In ZSYSTEM.ZPROCESS create a new instance, such as DMASTATS.
    - Specify the Method attribute as:  
**ZSYSTEM.ZMETHOD.PUTPROF\_DMASTATS**
  - 2 In ZSYSTEM.ZMETHOD create a new instance, such as PUTPROF\_DMASTATS.
    - Specify the Parameter attribute as:  
**DMASTATS**
    - Specify the Method Name attribute as:  
**EDMMPPRO**
-  Each execution of Distributed Configuration Server might generate several reporting objects at various points in the processing (see the section, DMASTATS). Each of these reporting objects will overwrite the previous one.
- In order to see every reporting object, configure ZSYSTEM.ZPROCESS.DMASTATS to invoke a customized REXX method.

## DMASTATS

Table 13 defines the fields of the DMASTATS object.

**Table 13: DMASTATS Fields Defined**

Field	Definition
BATCHDAT	Date of this report
BATCHTIM	Time of this report
BATSTDAT	Date of correlated starting (id=1) report
BATSTTIM	Time of correlated starting (id=1) report
BATCHRC	Character return code (if REPORTID > 1) Notes: See Table 14 on page 92 for REPORTID values. See Table 15 on page 93 for detailed BATCHRC information.
BATCHMSG	Completion message (if REPORTID > 1) Note: See Table 14 on page 92 for REPORTID values.

<b>Field</b>	<b>Definition</b>
BATARGS	DMABATCH command line
BATLKSTA	Result of <b>DMABATCH ACTION=LOCKSTATUS</b> : U (Unlocked) S (Soft-locked) X (Exclusive Soft-locked) H (Hard-locked)
DMASTATE	0 = Initial 1 = Compared 2 = Downloaded 3 = Committed
ZSRCMGID	Source MGR_ID
ZDSTMGID	Destination MGR_ID
REPORTID	Identifies which Distributed Configuration Server processing point sent the report. Note: See Table 14 below for detailed REPORTID information.
SCOPE	Scope of synchronization=DOMAIN
ZDOMAINS	List of domains
ZUSERID	User name for use with PUTPROF method (see ZUSERID on page 93)

Table 14 identifies which DMASTATS.REPORTID processing point sent the report.

**Table 14: REPORTID Values Defined**

<b>REPORTID</b>	<b>Definition</b>
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 15 lists the return codes that can be expected from DMASTATS, and what each means.

**Table 15: BATCHRC Values Defined**

BATCHRC	Definition
000	Completed OK.
003	Distributed Configuration Server timed-out waiting for tasks to end.
001-090	Configuration Server errors. See the Configuration Server log.
099	Client internal errors. See the Distributed Configuration Server log.
111	ACTION=RESET failed.
112	ACTION=DBVERIFY failed.
113	Differencing failed.
212	Client timeout.
218	Unable to establish communications to a Configuration Server.
999	Synchronization in progress (when REPORTID < 6).

## ZUSERID

If a value is specified for **Profile name** on the General tab, 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 no value is specified for **Profile name**, the default, <generate default>, will be used. In this case, ZUSERID is generated based on one of the following.

- If:

SCOPE=DOMAIN

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 batch operation:

DMA\_<target\_id>\_<action>

DMABATCH ACTION=LOCKSTATUS MGRID=123

generates

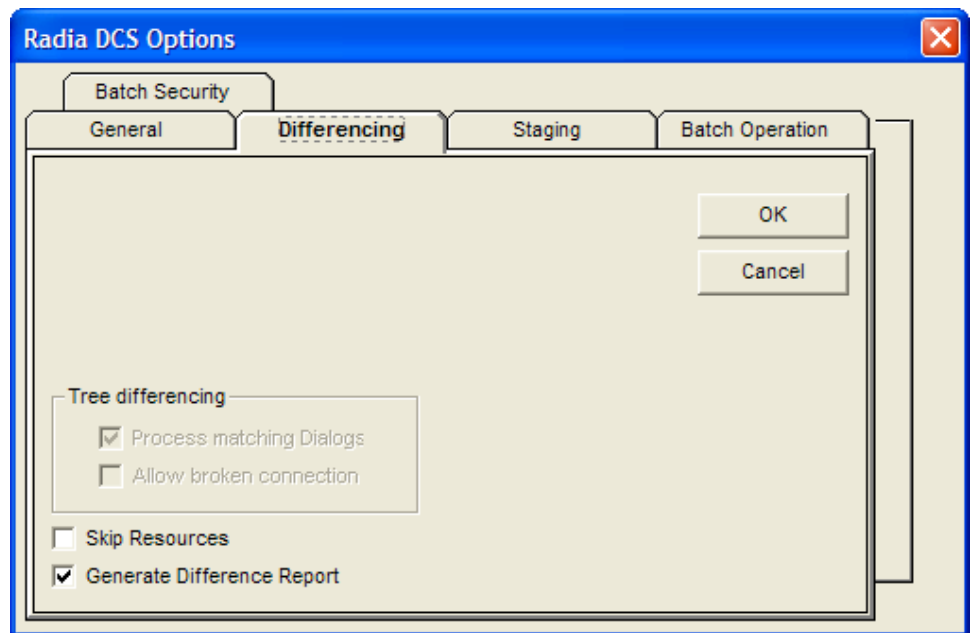
DMA\_123\_LOCKSTATUS



*target\_id* can be independent of *src\_id* and *dst\_id*.

## Differencing Options

With the Differencing options, an administrator can specify whether to enable resource skipping and report generation.



**Figure 6: Distributed Configuration Server Options: Differencing options.**

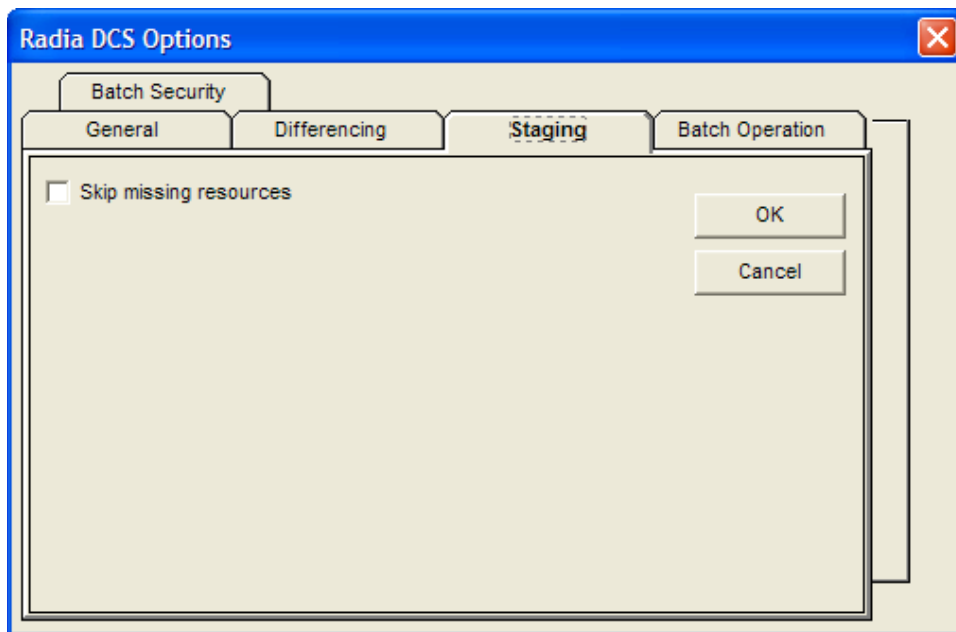
Table 16 describes the Differencing options.

**Table 16: Differencing Options**

Option (Object Variable)	Settings (defaults in bold)	Description
Skip Resources (NORES)	<b>0=use resources</b> 1=skip resources	This is an option to ignore resources during differencing.
Generate Difference Report (DIFFREPT)	0=disable <b>1=enable</b>	Enabling this option will result in a report of the database differencing being generated.

## Staging Options

On the Staging panel, an administrator can instruct Distributed Configuration Server whether to overlook missing database resources.



**Figure 7: The Distributed Configuration Server Options: Staging options.**

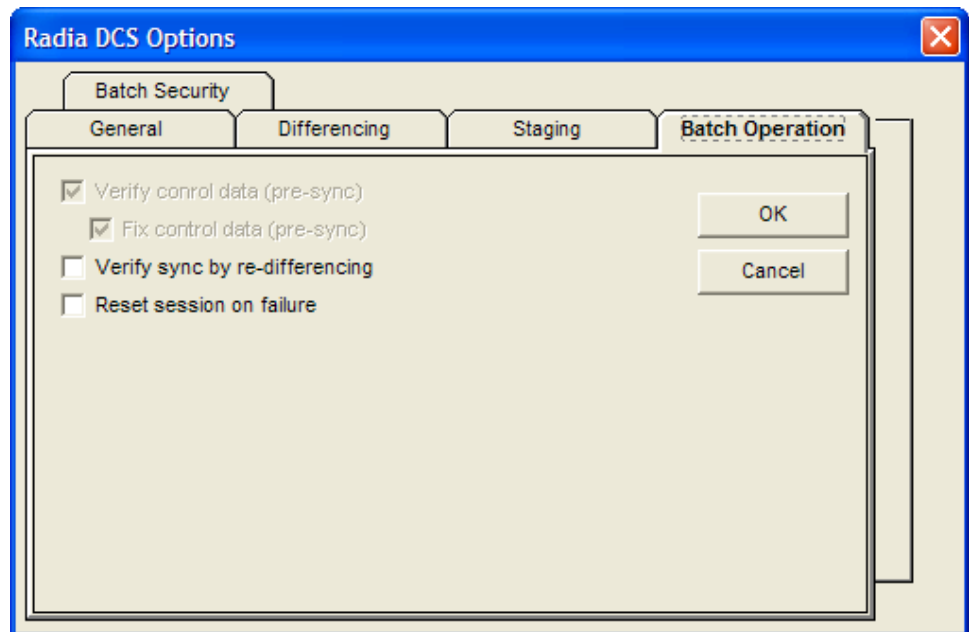
Table 17 describes the options that are available on the Staging panel.

**Table 17: Staging Options**

Option (Object Variable)	Settings (defaults in bold)	Description
Skip Missing Resources (SKIPMISS)	1=enable <b>0=disable</b>	Skips missing resources. Note: By default, if the Staging step does not find a resource on the Source, it will terminate. This option allows Staging to skip the resource and continue.

## Batch Operation Options

The Batch Operation options allow an administrator to enable or disable synchronization verification and session resetting.



**Figure 8: The Distributed Configuration Server Options: Batch Operation options.**

Table 18 describes the Batch Operation options.

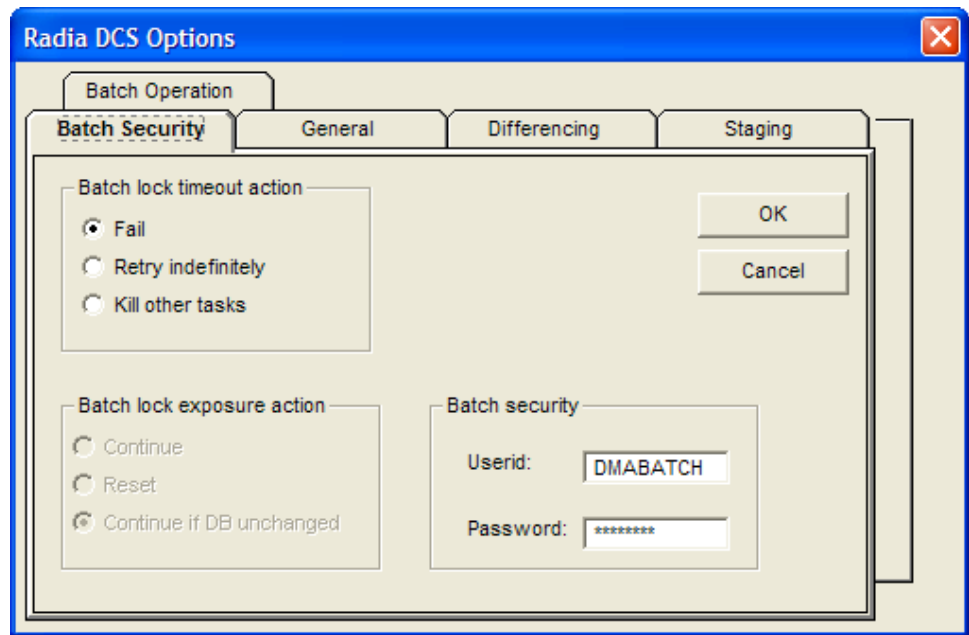


**Table 18: Batch Operation Options**

<b>Option (Object Variable)</b>	<b>Settings (defaults in bold)</b>	<b>Description</b>
Verify Control Data	N/A	This option is disabled.
Fix Control Data	N/A	This option is disabled.
Verify Synch by Re-differencing (SYNCHVFY)	<b>0=disabled</b> 1=enabled	Verify the synchronization results by re-running the differencing. If any additional differences are found, it restarts the process, and the differences are, in turn, transferred to the Destination.
Reset Session on Failure (BATRESET)	<b>0=disabled</b> 1=enabled	If synchronization fails, reset it to its initial status. Notes: Normally, if synchronization fails during staging (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 means leaving both Configuration Servers locked. If leaving the Configuration Servers locked, pending a restart, is not acceptable, this option allows the session to be reset to the initial state, and immediately unlocks both Configuration Servers, releasing staged resources. Any subsequent synchronization of this synchronization pair will start from scratch; if staging failed near the end of a long process, all of that processing is lost.

## Batch Security Options

With the Batch Security options an administrator can specify database-lock actions and security settings.



**Figure 9: The Distributed Configuration Server Options: Batch Security options.**

Table 19 describes the options available on the Batch Security panel.

**Table 19: Batch Security Options**

Option (Object Variable)	Settings (defaults in bold)	Description
Batch Lock Timeout Action (BATLOKTO)		Specify what to do in the event of a batch-lock timeout.  Note: A batch-lock timeout occurs when active non-Distributed Configuration Server tasks running on the Destination Configuration Server prevent Distributed Configuration Server from achieving a hard-lock at the Commit step.
Fail	<b>X – (Fail)</b>	Cancel the current database-lock attempt and report a BATCHRC=003.
Retry Indefinitely	R – (Retry)	Continue retrying until a database hard-lock is obtained.

<b>Option (Object Variable)</b>	<b>Settings (defaults in bold)</b>	<b>Description</b>
Kill Other Tasks	F – (Force)	Terminate all non-Distributed Configuration Server tasks that are running, obtain the hard-lock, and continue processing.
Batch Lock Exposure Action		This option is disabled—its behavior is hard-coded to <b>Continue if DB unchanged</b> .
Batch Security		
User ID (BATUSER)	<b>(DMABATCH)</b>	User ID for all Configuration Servers in batch mode.
Password (BATPWD)	<b>(DMABATCH)</b>	Password for all Configuration Servers in batch mode.



---

## 7 Distributed Configuration Server's DMABATCH

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

- The DMABATCH command-line arguments that can be used in a script that executes DMABATCH and handles error conditions
- The time-saving automated solutions that can automatically handle error and non-error situations during Distributed Configuration Server batch processing
- The DMABATCH synchronization-message variable, BATCHMSG, and return-code variable, BATCHRC, that are found in the ZMGRSYNC object

## Overview

DMABATCH is called by the executable file, `DMABATCH.EXE`. It requires no arguments and completes the database synchronization using the information that was specified in the Choose Configuration Servers and domains panel of the Distributed Configuration Server configuration-only phase.



The configuration-only information was saved in the `ZMGRSYNC` object on the Destination.

## DMABATCH Considerations

Before DMABATCH can be run, it must be configured in the Choose Configuration Servers and domains panel, as discussed starting on page 80.

- The pair of Configuration Servers (and selected domains) that was defined in the Choose Configuration Servers and domains panel will be synchronized.
- The associated Distributed Configuration Server log file and objects will be created in `IDMLOG` and `IDMLIB`, respectively, or the default directory for Distributed Configuration Server. The log file is `DMABATCH.LOG`.

## 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 [MANAGER=*id*][QTYPE=TASK | TRANS]

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

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

### DMABATCH ACTION=RESUME [MANAGER=*id*]

This command ends a “quiescent” state on the Destination.

- If MANAGER= is omitted, the default is the Destination's ID.

### DMABATCH ACTION=KILLTASKS [MANAGER=*id*]

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

- If MANAGER= 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, release any locks held by the session, 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 can't be left locked.

DMABATCH ACTION=SOFTLOCK [MANAGER=id]

DMABATCH ACTION=UNLOCK [MANAGER=id]

This pair of commands is 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 MANAGER= is omitted, the default is the Destination's ID.

## DMABATCH Automation

Distributed Configuration Server can be set up to automatically handle a variety of situations. The following are examples of error and non-error situations that might arise during Distributed Configuration Server's batch processing; and for which, automated solutions can save time and administrator intervention.

### Error Situations

- The synchronization is interrupted due to a physical (for example, line dropped) or logical problem. Should the databases remain locked?
- The synchronization is resumed after an interruption, but the Configuration Server has been recycled in the interim, with its database possibly exposed to updates. Should the synchronization resume or start over?  
See Reset Session on Staging Failure on page 105.
- At commit time, the Destination database cannot be hard-locked because non-Distributed Configuration Server client tasks are running. Should the Distributed Configuration Server wait for the tasks to end, terminate them, or fail?  
See Batch Lock Timeout Action on page 106.



## Non-Error Situations

- When it's time to commit the changes, the Destination must be hard-locked in order to deny access to data that is partially updated. However, this cannot occur while client tasks are running on it. The Destination waits ([MGR\_DMA].DMA\_TIMEOUT) for these tasks to end before aborting them, generating BATCHRC=003. See Batch Lock Timeout Action on page 106.
- If a partially completed synchronization terminates, and cannot be brought to completion quickly, its state will need to be reset, freeing the Configuration Server locks and other resources. See Reset Session on Staging Failure below.
- If one of the Configuration Servers being synchronized becomes unlocked before the operation is completed, should the synchronization be allowed to resume, or be forced to start over? See Batch Lock Timeout Action on page 106.

## Automated Solutions

This section details the set of Distributed Configuration Server options that can be specified in order to control DMABATCH's actions when an error occurs. These options can be stand-alone executions of DMABATCH with special command-line arguments.



These options are also available via the Distributed Configuration Server Options tabs.

The following options can be specified to affect how a single execution of DMABATCH will respond to certain error conditions. These options can be set to control DMABATCH operation without the use of a script.

### Reset Session on Staging Failure

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. Both Configuration Servers will be unlocked, and staged resources will be freed immediately. The trade-off is that "re-startability" is sacrificed, which can be a problem if staging failed near the end of a long process.

To manually reset a failed session

- Specify:

**DMABATCH ACTION=RESET**



This is equivalent to selecting **Reset session on failure** on the **Batch Operation** tab.

## Batch Lock Timeout Action

This option controls which of three possible actions Distributed Configuration Server will take if active non-Distributed Configuration Server tasks are running, and preventing the Destination from achieving a hard-lock at the Commit step.

**Table 20: Batch Lock Timeout Actions**

Action	Result
Fail	This is the default. It cancels the current attempt, and reports a BATCHRC=003.
Retry Indefinitely	Continue retrying until a lock is obtained.
Kill Other Tasks	Terminate all non-Distributed Configuration Server tasks that are running on the Configuration Server. Distributed Configuration Server obtains the hard-lock and continues commit processing.

To manually set a Batch Lock Timeout option

- Specify:

**DMABATCH ACTION=Fail|Retry|Force**



This is equivalent to selecting **Fail**, **Retry indefinitely**, or **Kill other tasks** in the **Batch Lock Timeout Action** section on the **Batch Security** tab.

## DMABATCH Command-Line Options

### Deferred Commit

If COMMIT=NO is specified,

#### **DMABATCH COMMIT=NO**

all Distributed Configuration Server processing is halted after the Staging step.

- 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 is unlocked and the Destination is soft-locked. The commit must be done subsequently without COMMIT=NO.

## IP Address Support for Cloned Managers

Cloned Managers share a database and a MGR\_ID. They are distinguishable only by IP name/address; and only one of the Configuration Servers “owns” the database. Only the owning Configuration Server can update and synchronize the database. To distinguish between cloned Managers for non-synchronization actions, on the command line, specify:

**RCSADDR=ipaddress**

(The MGR\_ID still needs to be specified.)

The ZMANAGER entry that matches the ID will supply all the other communications parameters. For example:

```
DMABATCH ACTION=SOFTLOCK MGRID=123 RCSADDR=local_host
```

## Hard-lock Operation

By specifying,

**DMABATCH ACTION=HARDLOCK**

the specified Configuration Server is hard-locked, thereby preventing clients from connecting. Also, any client 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 with Cloned Managers (see IP Address Support for Cloned Managers, above) that must be prevented from receiving connects while the database-owning Configuration Server is being synchronized.



For more information on the lock-status options, refer to the Version 4.4 Release Notes.

## 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, in the ZMGRSYNC object. At the Differencing step, a BATCHRC of 000 indicates that no domain differences were found. The associated BATCHMSG message is No domain differences found.

During the Staging and Commit phases of Distributed Configuration Server, the 000 return code indicates that the phase was successful. The corresponding BATCHMSG is `Synch OK`.

## Configuration Server Response to Distributed Configuration Server Request

Table 21 lists the Configuration Server BATCHRC and corresponding BATCHMSG responses to Distributed Configuration Server requests.

**Table 21: BATCHRC and BATCHMSG Responses**

BATCHRC	BATCHMSG
000	“No domain differences found.” (At the level indicated.)
000	“Synch OK.” Differences were found and the synchronization was successful.
001	“General warning.”
002	“Database is locked. Some client tasks were forced to end.”
003	“DCS timeout expired.”
005	“Timestamp mismatch. Unable to execute the transaction.”
009	“Lock timestamp must be specified. DMALTS is wrong or missing.”
010	“_Handle must be specified. It is wrong or missing.”
011	“DMA_Handle verification failure.”
012	“Invalid request object missing var(s).”
013	“userID/Password verification error. Transaction terminated.”
014	“Processing started.”
015	“Unknown function.”

<b>BATCHRC</b>	<b>BATCHMSG</b>
016	“DMA general error.”
017	“DMA mgr softlocked (shared).”
018	“DMA mgr hardlocked.”
019	“DMA mgr not locked.”
020	“DMA wrong mgr id.”
021	“Configuration Server is Standalone.”
022	“Stage file write err (out of space?).”
023	“Stage file read err.”
024	“Stage file iocontrol err.”
025	“Cntrl file write err (out of space?).”
026	“Cntrl file read err.”
027	“Cntrl file iocontrol err.”
028	“Database CreateInst failed (out of space?).”
029	“Database LockInst failed.”
030	“Database WriteInst failed (out of space?).”
031	“Database DeleteObj failed.”
032	“Database locked by more than one task.”
033	“Configuration Server is softlocked (exclusive).”
034	“Userid not defined to Configuration Server.”
035	“Stage directory not found.”
036	“Stagefile delete failed.”
037	“Stage directory delete failed.”
038	“Inconsistent lock state.”



---

# A Troubleshooting the Distributed Configuration Server

At the end of this appendix, you will know:

- some of the ways to troubleshoot Distributed Configuration Server, including:
- How to activate tracing for Distributed Configuration Server operations
- Which EDMAMS verbs are associated with Distributed Configuration Server, and how they are used
- How to prevent and correct domain-eligibility issues

## Logs to Obtain

For Distributed Configuration Server problems, `DMABATCH.LOG`, `DCS.LOG`, `DCSBATCH.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 shown below correspond to the domain-eligibility rules. Depending on the circumstances of the failed synchronization, these messages might be found in the `DMABATCH.LOG`, the `DCSBATCH.LOG`, or the `DCS.LOG` as detailed in this section.

- Version 4.7.1 messages are generated by Distributed Configuration Server synchronization processing, and will be found in `DMABATCH.LOG`.
- Version 4.6 messages are generated by the user interface- or batch-initiated (`DCSBATCH.EXE`) synchronization processing, and will be found in `DCS.LOG` or `DCSBATCH.LOG`, respectively.
  - The “last synch” and “last update” dates refer to the local time on the Destination Configuration Server.
  - The bracketed numbers [999] and [222] indicate the `MGR_ID`.

**Table 22: Domain-Eligibility Error Messages**

Version 4.7.1 Message	Version 4.6 Message
Skipping Domain [domain] because owners at source <src-id> and destination <dest-id> do not match	NVD002223 99069 16:48:06 Domain [SYSTEMX] not eligible: self-owned at Destination [999]
Skipping Domain [domain] because cannot synchronize to owner	NVD002223 99069 16:48:06 Domain [NEWDOMAN] not eligible: replication to owner [999]
Skipping Domain [domain] because owners at source <src-id> and destination <dest-id> do not match	NVD002223 99069 16:49:18 Domain [SYSTEMX3] not eligible: Source owner [222] and Destination owner [999] unequal



Version 4.7.1 Message	Version 4.6 Message
Skipping Domain [ <i>domain</i> ] because non-authoritative replica: updated (< <i>date</i> > < <i>time</i> >) since last synchronization (< <i>date</i> > < <i>time</i> >)	NVD002223 99069 16:50:18 Domain [SYSTEMX2] not eligible: peer mode and Source was updated [97/12/17 19:42:26] after its last synch [97/12/01 12:00:00]
Skipping Domain [ <i>domain</i> ] because possible DB regression - destination replica (< <i>date</i> > < <i>time</i> >) more recent than source (< <i>date</i> > < <i>time</i> >)	NVD002223 99069 16:52:18 Domain [SYSTEMX2] not eligible: peer regression: last dest update [99/12/18 19:42:26] more recent than last Source update [99/12/13 19:42:26]

## Log and Object Locations

The default locations for the Distributed Configuration Server objects and logs are IDMLIB and IDMLOG, respectively.

## Configuration Server Tracing for Distributed Configuration Server

In the MGR\_TRACE section of the edmprof file, add the following setting and value:

**DMA=YES**

## Distributed Configuration Server Objects and Files

### Distributed Configuration Server Objects

Obtain the following objects from the default Distributed Configuration Server directory. If Distributed Configuration Server is running on a desktop with either a Radia client or Administrator Workstation, look in IDMLIB.

- ZMANAGER contains the properties of all the Configuration Servers that have been defined to Distributed Configuration Server. 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 Distributed Configuration Server 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 21 on page 108.

## Distributed Configuration Server Files

This section defines the Distributed Configuration Server's .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 Radia database file operations.

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

### .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 Radia database objects. The verbs, keywords, and values can be specified in uppercase, lowercase, and mixed-case.



For more information on the EDMAMS verbs, refer to the *Configuration Server Guide*.

Three of the EDMAMS verbs will display or update Distributed Configuration Server control data:

## REFRESH\_DMA

This verb rebuilds instance counts, class counts, and update dates in the database-control data.

- If **DOMAIN** is omitted, all domains are refreshed.

```
ZEDMAMS VERB=REFRESH_DMA(,PREVIEW=YES/NO)(,DOMAIN=domain_name)(,CLASS=class_name)
```

## UPDATE\_MGRIDS

This verb updates the MGR\_ID, Configuration Server name, owning MGR\_ID, and owning Configuration Server name in the database-control data.

- 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_mgr_name)(,MID=local_mgr_id)(,MMNAME=owning_mgr_name)(,MMID=owning_mgr_id)
```

## LIST\_PREFIX

This verb displays formatted database-control data.

If **DOMAIN** is omitted, all domains are displayed.

If **CLASS** is omitted, all classes are displayed.

```
ZEDMAMS VERB=LIST_PREFIX(,FILE=file_name)(,DOMAIN=domain_name)(,CLASS=class_name)
```

Output is written to `ZEDMAMS.LOG`, with the exception of error conditions, which are written to `STDERR`.

## Domain Eligibility

- *What if Distributed Configuration Server presents no domains as eligible for synchronization?*

If no domains are presented as eligible for synchronization, make sure that both Configuration Servers were installed properly—as Distributed Configuration Server-enabled Configuration Servers—because domain ownership is assigned during installation.



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

- *Which Configuration Server owns the default domains (SYSTEMX, ZACCESS, and ZSYSTEM)?*

If Configuration Server 001 owns them, make sure that they were not assigned ownership to Configuration Server 002 during its installation.

# Index

.

.dat files, 114

.idx files, 114

.mk files, 114

## A

ADMIN\_LIST, 69

## B

batch automation, 104

BATCHRC, 93, 103

    values defined, 93

BATLOKTO, 98, 106

BATPWD, 99

BATRESET, 97

BATUSER, 99

## C

Cloned Manager, 19, 74, 107

Configuration Server

    IP name/address, 80

    lock-status, 80

    operations, 79

    properties, 73

        default values, 74

        table, 74

    shared IDs, 80

    synchronization eligibility, 25

Configuration Servers, defining to Distributed  
    Configuration Server, 71

    copying, 75

configuring Distributed Configuration Server, 30

container file, 19, 32

copying Configuration Servers within Distributed  
    Configuration Server, 75

current MGR\_ID, 25

customer support, 4

## D

DCS.LOG, 112

DCSBATCH.LOG, 112

Destination component, 24

    installation, 49

    temporary directory, 63

Destination Configuration Server

    domain selection

        automatic, 82

        dynamic, 83

        manual, 82

    installation, 49

DIFFREPT, 95

directories

    Distributed Configuration Server, 37

Distributed Configuration Server

    adding Configuration Servers, 72

    commit changes, 33

    communications protocol, 36

    copying Configuration Servers, 75

    defining Configuration Servers, 32, 71

    deleting Configuration Servers, 76

    description, 22

    Destination component installation, 49

    Destination Configuration Server, 23

    directories, 37

    domain eligibility rules, 28

        log error messages, 112

    domain selection, 82

    download and transfer resources, 33

    download resources, 33

    installation

        Destination, 49

- Source, 43
- installation options, 36
  - Destination component, 36
  - Source component, 36
- logs, 30, 112
  - Configuration Server logs, 112
  - DCS.LOG, 112
  - DCSBATCH.LOG, 112
  - DMABATCH.LOG, 112
  - log error messages, 112
- logs and objects, 30
- menu options, 77
- navigation buttons, 77
- objects, 30
  - saved, 114
  - ZMANAGER, 114
  - ZMGRSYNC, 102, 114
- options, 88
  - Batch Operation, 96
    - post-synchronization verification, 96
    - session resetting, 96
  - Batch Security, 97
    - database-lock actions, 97
    - security settings, 97
  - Differencing, 94
    - report generation, 94
    - resource skipping, 94
  - General, 88
    - domain validation, 88
    - logging, 88
    - status reporting, 88
  - Staging, 95
    - skip missing database resources, 95
- options tabs, 88
  - Batch Operation, 96
  - Batch Security, 97
  - Differencing, 94
  - General, 88
  - Staging, 95
- options, setting, 88, 94, 95, 96, 97
- processes, 31
- processor requirements, 36
- recommendations and requirements, 36
- resources
  - download, 33
  - transfer, 33
- saved objects, 114
- security, 66
  - Configuration Server security settings, 68
  - password, 66
  - setting up, 66
  - user ID, 66
- selecting synchronization domains, 32
- Source component installation, 43
- Source Configuration Server, 23
- space requirements, 39
- steps
  - commit, 33
  - defining Configuration Servers, 32
  - domain selection, 32
  - download and transfer resources, 33
  - download resources, 33
  - selecting domains, 32
  - synchronization setup, selecting domains, 32
  - transfer resources, 33
- supported operating systems, 37
- synchronization setup, select domains, 32
- terminology, 18
  - Cloned Manager, 19
  - container file, 19
  - Destination Configuration Server, 18
  - domain ownership, 18
  - foreign-owned domain, 19
  - middle-tier Configuration Server, 19
  - peer synchronization, 18
  - self-owned domain, 19
  - Source Configuration Server, 18
  - synchronization, 18
  - synchronization pair, 18
  - unrelated domains, 19
- transfer resources, 33
- version information, 77
- Distributed Configuration Server-specific terminology, 18

- DMABATCH, 102
  - automated solutions, 105
  - automation options
    - batch lock timeout action, 106
  - IDMLIB, 102
  - IDMLOG, 102
  - kill tasks, 103
  - quiesce, 103
  - reset, 104
  - resume, 103
  - softlock, 104
  - unlock, 104
- DMABATCH.EXE, 30, 102
- DMABATCH.LOG, 102, 112
- DMASTATS, 91
  - BATCHRC, 93
  - fields defined, 91
  - REPORTID, 92
- document map, 16
- domain eligibility, 28
- domain eligibility rules, 28
  - domain deletion, 28
- domain naming considerations, 26
- domain validation, 90
- domains
  - current MGR\_ID, 25
  - domain name, 25
  - eligibility, 28
    - rules, 28
  - foreign-owned, 26
  - local updates, 29
  - owning MGR\_ID, 25
  - self-owned, 25
  - unrelated, 29

## E

- EDMAMS, 115
  - LIST\_PREFIX, 115
  - REFRESH\_DMA, 115
  - UPDATE\_MGRIDS, 115
- edmprof file, 69, 84
  - MGR\_DMA, 85

- MGR\_STARTUP, 84
- MGR\_TRACE, 113
- EDMSIGN, 69
- eligibility, domains, 28
- eligible domains, 32

## F

- files
  - .dat, 114
  - .idx, 114
  - .mk, 114
- foreign-owned domain, 26

## I

- IDMLIB, 102, 113
- IDMLOG, 102, 113
- Integration Server, 24

## K

- kill tasks, 103

## L

- local updates, 29
- LOGSIZE, 89
- LOGWRAP, 89

## M

- MGR\_DMA, 68, 84, 85
  - DMA\_TIMEOUT, 86
  - SECURITY\_METHOD, 69
- MGR\_ID, 25
- MGR\_STARTUP, 84
  - MANAGER\_TYPE, 84
  - MGR\_ID, 85
  - MGR\_NAME, 84
  - TCP\_PORT, 85
- MGR\_TRACE, 113

## N

- NORES, 95

## O

owning MGR\_ID, 25

## P

pre-installation notes, UNIX, 39

processor requirements

    Distributed Configuration Server, 36

PUTPROF, 91

## Q

quiesce, 103

    qtype, 103

    task, 103

    trans, 103

## R

RDCS Batch desktop icon, 30

RDCS Configuration desktop icon, 5

REPORT, 90

REPORTID, 92

    values defined, 92

REPTNAME, 90

reset, 104

resume, 103

## S

saved Distributed Configuration Server objects, 114

security on the Configuration Server, 69

security, setting up in Distributed Configuration Server, 66

SECURITY\_METHOD, 69

self-owned domain, 25

setting up security in Distributed Configuration Server, 66

shared MGR\_ID, 74

simultaneous synchronizations, 30

SKIPMISS, 96

softlock, 104

Source component, 23

    installation, 43

    temporary directory, 63

Source Configuration Server

    installation, 43

status reporting, 90

STDERR, 116

STRICT, 90

strict domain validation, 90

supported operating systems

    Distributed Configuration Server, 37

synchronization pair, 25

    control information, 22

    ZMGRSYNC, 114

synchronization, domain eligibility, 28

SYNCHVFY, 97

## T

technical support, 4

-temp-dir, 63

temporary directories, 63

    Destination, 63

    Source, 63

    -temp-dir, 63

    TMPDIR, 63

terminology, 17

    Distributed Configuration Server, 18

    Integration Server, 18

TMPDIR, 63

troubleshooting Distributed Configuration Server

    Configuration Server property information, 114

    default domain ownership, 116

    Distributed Configuration Server logs, 112

    domain eligibility, 116

    EDMAMS utility, 115

        LIST\_PREFIX, 115

        REFRESH\_DMA, 115

        UPDATE\_MGRIDS, 115

files

    .dat, 114

    .idx, 114

    .mk, 114

IDMLIB, 113

IDMLOG, 113

INI files, 113



- no eligible domains, 116
- synchronization pair information, 114
- tracing, 113

## U

- UNIX pre-installation notes, 39
- unlock, 104
- unrelated domains, 29

## Z

- ZCOMTYPE, 74
- ZEDMAMS log, 116
- ZMANAGER, 114
  - Configuration Server property information, 114
- ZCOMTYPE, 74
- ZMGRID, 74
- ZMGRNAME, 74
- ZTCPADDR, 75

- ZTCPADDR, 75
- ZTIMEO, 74
- ZMGRID, 74
- ZMGRNAME, 74
- ZMGRSYNC, 102, 114
  - BATCHMSG, 101, 108
  - BATCHRC, 101, 108
  - BATLOKTO, 106
  - Distributed Configuration Server sessions saved, 114
  - synchronization pair saved, 114
- ZTCPADDR, 75
- ZTCPADDR, 75
- ZTIMEO, 74
- ZTRACEL, 89
- ZUSERID, 92, 93

