DataHub for UNIX Operating Systems

SC26-8669-01

Installation and Configuration Guide

Release 2

IBM

DataHub for UNIX Operating Systems

SC26-8669-01

Installation and Configuration Guide

Release 2

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices" on page v.

Third Edition (May 1996)

This edition replaces and makes obsolete the previous edition, SC26-8669-0. The technical changes for this edition are summarized in "Summary of Changes" on page xii, but because the changes are extensive, they are not indicated by vertical bars in the left margin.

This edition applies to Release 2 of DataHub for UNIX** Operating Systems, 5765-530, and to any subsequent releases until otherwise indicated in new editions or technical newsletters. Make sure you are using the correct edition for the level of the product.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers' comments is provided at the end of this publication. If the form has been removed, address your comments to:

IBM Corporation, Department J58
P. O. Box 49023
San Jose, CA 95161-9023
United States of America

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

Licensees of this program who wish to have information about it for the purpose of enabling (1) the exchange of information between independently created programs and other programs (including this one) and (2) the mutual use of the information that has been exchanged, should contact:

IBM Corporation, Department J01
P. O. Box 49023
San Jose, CA 95161-9023
United States of America

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AIX	DB2
AIX/6000	DB2/6000
AIXwindows	IBM
C Set++	NetView
DATABASE 2	RISC System/6000
DataHub	SystemView

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

About This Book

This book will help you install and configure DataHub for UNIX** Operating Systems.

The installation and configuration of DataHub is a team effort. One or more members of the team should have knowledge and skills in the administration of operating systems (AIX, HP-UX**, and Sun Solaris**), relational database systems (DB2, INGRES**, ORACLE**, SYBASE**), TCP/IP communications, and LAN environments.

Who Should Read This Book

This book is written for technical professionals, database administrators, system administrators, and users who are involved in planning, installing, configuring, and solving problems in a DataHub environment.

The readers for this book should know the basic functions of the UNIX operating environment where DataHub will be installed, including TCP/IP commands (**ftp** and **telnet**), and vi or another UNIX system file editor.

Readers of this book should also know the basic functions of the relational database management systems (RDBMSs) that will be used and managed by DataHub.

How to Use This Book

This book is divided into the following chapters:

- Chapter 1, “Preparing to Install and Configure DataHub” on page 1, provides information required before you install DataHub; it explains basic DataHub concepts as well as technical environment requirements. Read this chapter before you install and configure DataHub.
- Chapter 2, “Installing DataHub Control Point Files” on page 18, provides instructions for copying control point files from the installation media to your system.
- Chapter 3, “Building DataHub INGRES Components” on page 23, provides instructions for building and distributing DataHub files required for managing and monitoring INGRES databases.
- Chapter 4, “Configuring a DataHub Control Point” on page 26, provides instructions for configuring a DataHub control point with all components on one workstation. After completing this chapter, DataHub is available for operations.

- Chapter 5, “Configuring DataHub Components: Alternative Options” on page 43, provides advanced instructions for configuring DataHub components in complex environments. Use the instructions in this chapter if you need to configure a control point with components on more than one workstation.
- Chapter 6, “Installing DataHub Managed Host Files” on page 53, provides instructions for copying managed host files from the installation media to your system.
- Chapter 7, “Configuring a DataHub Managed Host” on page 59, provides instructions for configuring a DataHub managed host. After completing the instructions in this chapter, the configured host is available for management by your control point.
- Chapter 8, “Customizing Your DataHub Environment” on page 71, provides instructions for customizing DataHub′s appearance and enabling DataHub to work with other applications.
- Chapter 9, “Troubleshooting DataHub Conditions and Messages” on page 78, provides tips and hints useful if DataHub is not working properly.
- Chapter 10, “Removing DataHub from a Workstation” on page 92, provides information you need when un-installing DataHub files from workstations.

The book ends with several appendixes, a bibliography, a glossary, and an index.

Terminology

Table 1 on page ix provides a brief list of common DataHub terms and shortened names of several RDBMS types.

You can find definitions of DataHub terms in the text of this book. When the book introduces new terms, it italicizes and defines them. You can also find definitions in “Terms and Abbreviations” on page 104, which contains definitions of DataHub terms and technical terms that pertain to DataHub.

Table 1. DataHub Basic Terminology List

Term	Definition
AIX	Advanced Interactive Executive
DataHub	The DataHub for UNIX Operating Systems product
DB2	Refers collectively to: IBM DATABASE 2 for AIX/6000, Version 1 IBM DATABASE 2 for AIX, Version 2 Release 1 IBM DATABASE 2 for HP-UX, Version 2 Release 1 IBM DATABASE 2 for the Solaris Operating Environment, Version 2 Release 1
DB2 for AIX	IBM DATABASE 2 for AIX, Version 2 Release 1
DB2 for HP-UX	IBM DATABASE 2 for HP-UX, Version 2 Release 1
DB2 for Solaris	IBM DATABASE 2 for the Solaris Operating Environment, Version 2 Release 1
DB2 Version 1	IBM DATABASE 2 for AIX/6000, Version 1
DB2 Version 2	Refers collectively to: IBM DATABASE 2 for AIX, Version 2 Release 1 IBM DATABASE 2 for HP-UX, Version 2 Release 1 IBM DATABASE 2 for the Solaris Operating Environment, Version 2 Release 1
Host	A workstation operating system that DataHub can manage
HP	HP-UX
Managed database	A database that resides on a managed host and is managed by DataHub
Managed host	A host managed by DataHub
Mouse button 1	The left-hand button of a mouse when the mouse is configured for a right-handed user
Sun	Sun Solaris Operating Environment
Sybase database	A database under a SYBASE SQL Server**
Sybase server	SYBASE SQL Server

Conventions

This section identifies the typographic, special symbol, and command line entry conventions used in this book.

Typographic Conventions

This book uses the following typographical conventions:

Monospace font	Text shown in monospace font should be typed exactly as shown; for example, aixmh.tar.
Bold monospace font	Text shown in bold monospace font (commands and keywords) should be typed exactly as shown; for example, **lpstat**.
Italic font	Words shown in italics are new terms with definitions specific to DataHub. These words are defined in the glossary.
Italic monospace font	Text shown in italic monospace font represents a variable requiring substitution of an installation-specific value; for example, *archive_file*. Variables are used to represent strings of text that are dependent upon your particular configuration. If a chapter contains several variables, they are defined in the beginning of the chapter.

Symbol (Reverse Font) Conventions

Small black boxes surrounding text (reverse font) are used to identify steps for specific RDBMS or operating system types.

The black box symbols are:

Symbol	System
DB2	DB2 (all versions)
DB2v1	DB2 Version 1 only
DB2v2	DB2 Version 2 only
DB2AIX	DB2 for AIX only
DB2HP	DB2 for HP-UX only
DB2SUN	DB2 for Solaris only
Ing	INGRES
Ora	Oracle
Syb	Sybase (server or database)
AIX	IBM AIX
HP	HP-UX
Sun	Sun

Command Line Entries

This book shows sequences of command line entries that you must enter within the same step on separate lines. For example:

cd /u
mkdir *datahub_dir*

When a lengthy command line entry extends beyond the margin of the book, a backslash (\) is shown at the end of the line to indicate that the following line is a continuation of the current entry. Do not type the backslash continuation character as part of the command. For example:

export PATH=.:./bin:/usr/bin:/usr/local/bin:/usr/local/X11/bin:\
/usr/local/lpp/bin:$HOME/bin

Using This Book Online

This book is available in two formats on the installation media:

DHUI1200.INF You can display this INF file with the Information Presentation Facility (IPF) book viewer (xview). DataHub provides xview. To install and use xview, refer to "Installing IPF/X Softcopy Book Support for DataHub" on page 74.

DHUI1200.PS You can print this PostScript** file using a local PostScript printer.

Summary of Changes

This section lists product and document updates for Release 2.

Product Changes

Significant product additions include:

- Support for:
  - IBM DATABASE 2 for HP-UX, Version 2 Release 1
  - IBM DATABASE 2 for the Solaris Operating Environment, Version 2 Release 1
  - INGRES
- Grouping functions
- Enhanced filtering for objects displayed in the Object Tree window
- Find functions for locating objects in the Object Tree window
- Database discovery
- Enhanced watchdog functions
- ORACLE backup and recovery functions
- Migration support for current DataHub users

User′s Guide Changes

Significant book updates include:

- New sections for INGRES
- Documentation for grouping, filtering, find, database discovery, and watchdog functions

Installation and Configuration Guide Changes

Significant book updates include:

- Reorganized book structure
- Documentation for INGRES procedures and migration windows

Chapter 1. Preparing to Install and Configure DataHub

This chapter prepares you to install and configure DataHub. Read this chapter before performing any installation or configuration tasks.

DataHub Architecture and Components

DataHub helps you manage relational database management systems (RDBMSs) and operating systems. You can manage systems from either one central location or several locations throughout a network.

Before installing the product, you should know how DataHub will be used at your site. DataHub supports various methods of database systems management:

- Local management of local data

  All data is in the same physical location. The DataHub administrators might be responsible for authorizing new users, backing up data, restoring data in the event of a failure, copying data between databases, or monitoring the general status of databases.

- Central management of distributed data

  The data is located at more than one location. The role of the DataHub administrator expands to manage databases at multiple locations, including different databases on heterogeneous UNIX platforms. The administrator is responsible for all database administration, which includes monitoring the status of the databases, tracking the movement of data between systems, and other related tasks.

- Distributed management of distributed data

  Several administrators manage data in remote and central locations using DataHub workstations at more than one location. Remote administrators have full control over local data and some functions at the central site. Central administrators have full control over all data.

For all installations, DataHub uses Transmission Control Protocol/Internet Protocol (TCP/IP) as its standard communication protocol. TCP/IP allows DataHub to communicate with your systems locally and remotely. Authorized administrators using TCP/IP and the X Window System can run DataHub remotely from connected systems.

The DataHub Distributed Architecture

The DataHub architecture is optimized for a distributed environment with two or more workstations containing DataHub. The DataHub workstation types are:

- The *control point*—the programmable workstation from which you manage your local and remote hosts and databases.
- *Managed hosts*—the systems on which managed databases are installed.

See Figure 1 for an overview of the DataHub architecture.

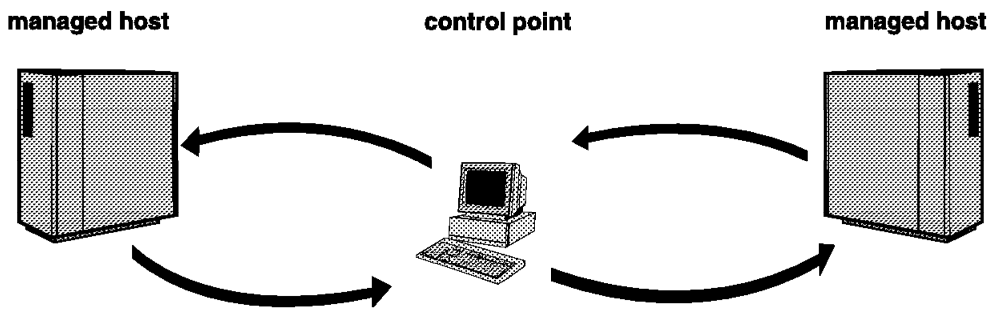

Figure 1. DataHub for UNIX Operating Systems Architecture

It is important to understand that the DataHub distributed management model typically comprises one control point and one or more managed hosts. The control point and managed hosts can have any number of databases of different RDBMS types residing on them.

The DataHub control point and managed hosts consist of a number of components. The DataHub distributed architecture applies to these components. The set of components comprising a control point can be on two or more workstations. And an administrator using DataHub can be on any host on the TCP/IP network where there is X Window System support.

When preparing for your installation, consider the ramifications (space, access, distance, and so on) of where you install DataHub components and how you access those components.

The DataHub Components

The DataHub components are:

- The *control point application*
- The *control database*
- The *watchdog server*

- *Operating system* and *database watchdogs*
- *Operating system* and *database drivers*

For definitions and detailed information on each component, read the following sections.

Control Point Application

The control point application contains the graphical user interface (GUI) and manages the DataHub environment.

The control point application communicates with operating system drivers and database drivers so you can monitor and administer managed hosts and databases.

If multiple control point applications share a control database, the view presented to each is consistent. Control point applications with separate control databases are not aware of each other′s control data. The control point workstation contains a control point application.

You can install a control point application on any of the platforms supported by DataHub.

Control Database

The control database contains the DataHub control tables. These tables hold:

- Information about the types of objects and actions that each user can view in the control point application
- Information about managed hosts and managed databases
- Watchdog checks to be run
- Check values that are optionally returned by the watchdogs
- Watchdog rules specifying conditions to evaluate and actions to take
- DataHub operational items

The control database typically resides on the workstation that is running the control point application. The control database, however, can reside on any host managed by DataHub.

The control database can be a DB2, INGRES, ORACLE, or Sybase database. You must create the DataHub control database (or select one that exists).

It is recommended that you do not share the control database with other applications.

Watchdog Server

The watchdog server is the collective name for a group of processes used by DataHub monitoring functions. For example, the watchdog server retrieves information from the control database about the *watchdog checks* (or *checks*, for short) to execute for each managed system. Checks are commands or scripts that run at set intervals and monitor the condition of a RDBMS or an operating system. The watchdog server sends the checks to managed host watchdog processes.

When results from checks exceed defined thresholds, check results are evaluated by rules. If the check results satisfy the conditions specified in a rule, the associated *action* for that rule is invoked. An action is a response to the condition defined in a rule. Actions can include sending an alert (with details of the condition) to a user, launching a program (typically to take preventative or corrective action), or sending an SNMP-trap to an SNMP management product (such as NetView).

Rule evaluation is done at a managed host if all checks used by the rule are from checks at that managed host. In this case, actions are initiated at the managed host without communication with the watchdog server.

If checks used in a rule are from two or more managed hosts, the results of the checks for that rule are forwarded to the watchdog server for global evaluation. A check can contain a request to store filtered values in the control database. Storing check values in the control database is optional. If the check values are to be stored in the database, each filtered value will be sent to the watchdog server for storage.

The watchdog server is typically located on the same workstation as the DataHub control database; however, it can reside on any host managed by DataHub.

Operating System and Database Watchdogs

There are two kinds of watchdogs. An *operating system (OS) watchdog* monitors conditions at a managed host; a *database watchdog* monitors conditions at a managed database system.

The checks that an OS watchdog executes (called *OS checks*) can include operating system commands, shell scripts, or other programs. The checks that a database watchdog executes (called *database checks*) can include SQL statements or database commands.

Typically, you want to monitor operating systems and databases. To do this, you must set up one OS watchdog on the control point workstation and on each managed host. Likewise, to monitor RDBMSs, you must set up database watchdogs at the control point and on each managed host for the types of RDBMSs that reside on that host.

> Each managed database instance or server (RDBMS) requires its own database watchdog; thus, you might require two or more database watchdogs on each workstation.

To monitor databases, you need:

DB2 One database watchdog for each instance on the workstation
INGRES One database watchdog for each II_SYSTEM directory
ORACLE One database watchdog for each ORACLE_HOME environment variable
Sybase One database watchdog for each Sybase directory

All watchdog checks are run under the authority of the user specified in the **Watchdog User** field during configuration of the watchdog.

Operating System and Database Drivers

Operating system drivers are the interfaces between the control point and the operating systems at both the control point workstation and managed host systems. All requests from the control point for operating system details are handled by the operating system drivers.

DataHub provides an operating system driver for each of the supported operating system types. There must be a DataHub operating system driver on the DataHub control point and each DataHub managed host.

Database drivers are interfaces between the control point and all managed databases. Requests for database details from the control point application are handled by the database drivers. All managed databases, including the control database, require the presence of a database driver.

DataHub provides a database driver for each of the supported RDBMS types. There must be a database driver for each database type on a particular host (control point and managed host).

> Only one driver is required for each type of RDBMS or operating system on each workstation.

A Typical DataHub Configuration

Figure 2 illustrates a typical installation: one control point workstation, two (or more) managed hosts, and watchdog checks defined for databases on the managed hosts.

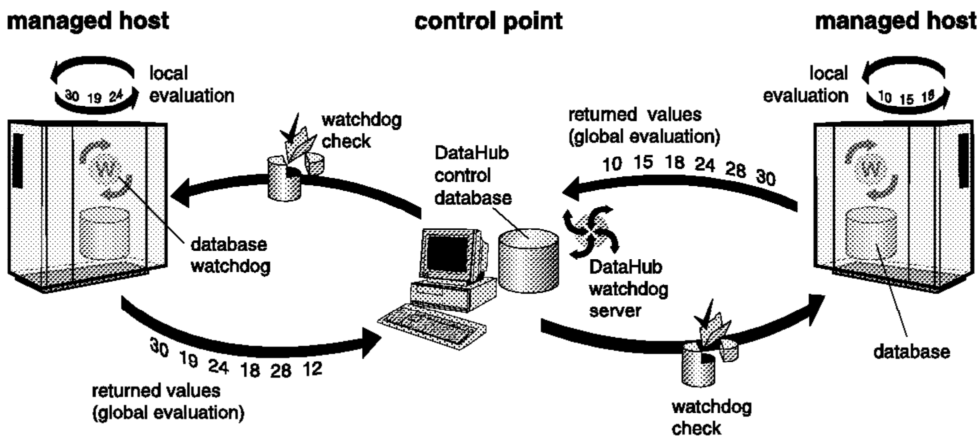

Figure 2. A Typical DataHub Installation

In this figure, the control point workstation contains all three major control point components: the control point application, the control database, and the watchdog server. The figure presents a centralized configuration for database system management. The figure also shows check values for a managed host being evaluated locally (where all checks in a rule are for checks at that managed host) and check values being returned to the watchdog server for global rules evaluation (where checks in a rule are for checks from two or more managed hosts). Check values are also returned to the watchdog server if the check definition specifies that values will be stored in the control database.

Typical Control Point Workstation Components

A typical DataHub control point contains several of the components discussed earlier in this chapter, including:

- A control point application
- A control database
- A watchdog server
- An operating system driver
- One or more database drivers
- An operating system watchdog

- One or more database watchdogs

The DataHub control point that you install and configure will probably look like the configuration in Figure 3. Alternative configurations are possible. "Alternative DataHub Configurations" on page 8 can help you decide if you want to consider a different approach.

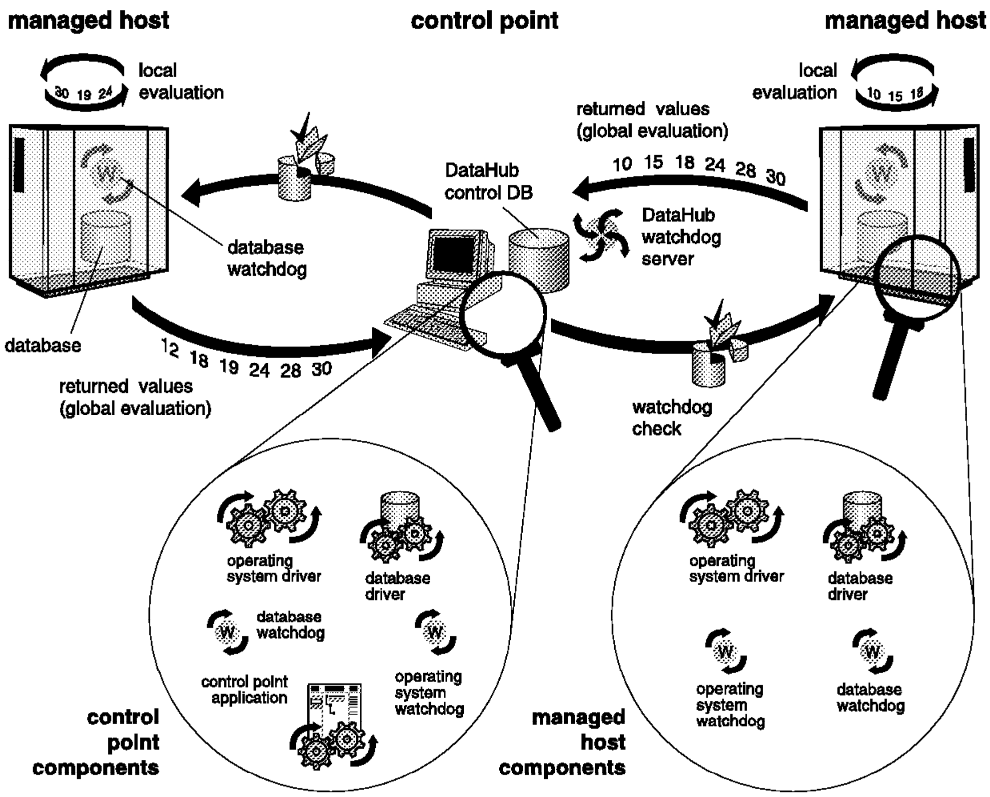

Figure 3. Control Point and Managed Host Component Details

Typical Managed Host Components

A typical DataHub managed host contains several of the components discussed earlier in this chapter, including:

- An operating system driver
- One or more database drivers
- An operating system watchdog
- One or more database watchdogs

Most or all of your managed hosts will contain these components.

You have finished reading about a typical DataHub configuration. Your environment might require an alternative configuration.

If the configuration explained in the last few pages will suit your requirements, skip to "Planning Your DataHub Installation and Configuration" on page 12. If the configuration explained in the last few pages seems appropriate but you want to manage two or more databases on a single system (control point or managed host), read "Monitoring Multiple RDBMS Instances." If you require a custom configuration, continue with "Alternative DataHub Configurations."

Alternative DataHub Configurations

This section explains some of the options available to you when installing DataHub. You can, if needed, build a customized DataHub environment component-by-component.

Supported options include:

- "Monitoring Multiple RDBMS Instances"
- "Setting Up a Remote Control Database" on page 9
- "Setting Up Multiple Watchdogs per Database Instance" on page 10

Monitoring Multiple RDBMS Instances

Each RDBMS instance (refer to the definition list on page 5 for more details) that you want DataHub to monitor must have its own watchdog. This requirement applies to databases of the same or of different RDBMS types, regardless of whether they reside on the control point or on a managed host.

A typical configuration, however, will configure only one RDBMS watchdog. If two or more RDBMSs exist on one workstation (shown in Figure 4 on page 9), additional steps are needed.

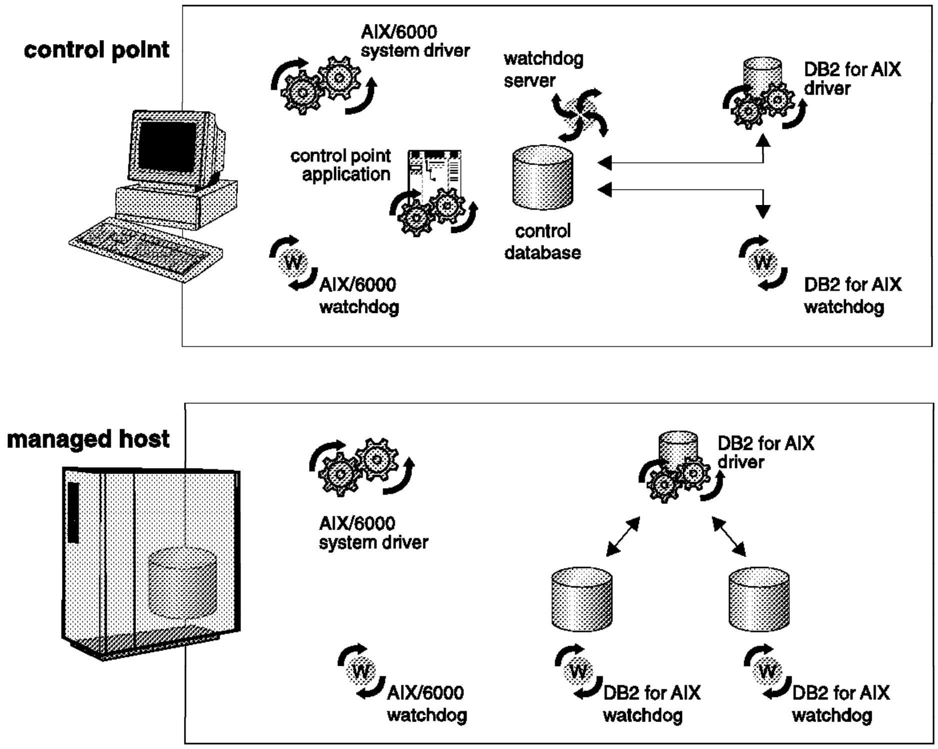

Figure 4. Sample Configuration with Multiple Database Instances of the Same RDBMS Type

First, you must install and configure the control point or managed host components. Later, you need to follow additional procedures and specify the information for each additional database instance. You can then configure as many database watchdogs as required to support your environment.

These additional procedures are covered in detail in "Configuring Watchdogs" on page 51.

Setting Up a Remote Control Database

In a typical DataHub environment, the control database and the control point application are on the same workstation. The control database and the control point application, however, can reside on different workstations. You might choose this alternative setup if you already have a dedicated database workstation and do not want to install another RDBMS on the control point workstation. Figure 5 on page 10 shows a remote control database setup.

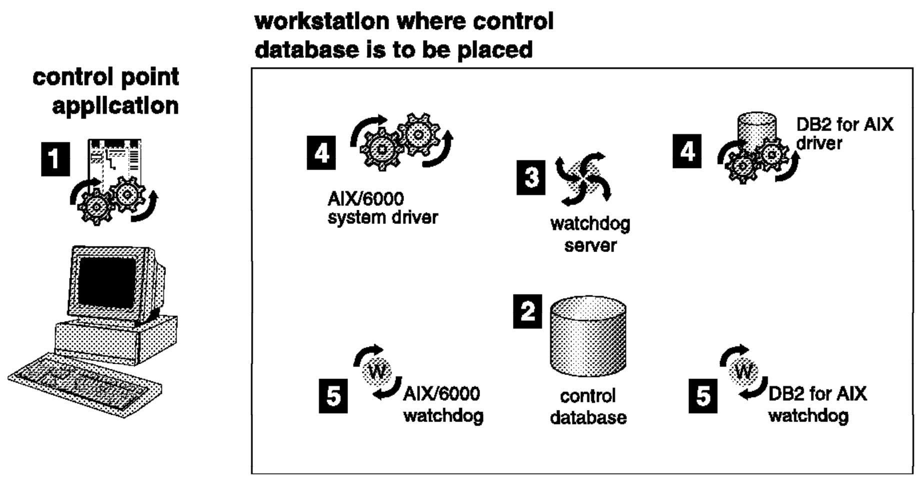

Figure 5. Sample Configuration with a Remote Control Database

A multiple control point configuration can offer increased efficiency for each database administrator, because separate control points can be used to access different control databases at different times. Also, depending on the division of responsibilities among the administrators, separating the control databases from the control points allows for more efficient use of processing power among different systems.

To install and configure the control database separately from the control point application, you will need to configure each component separately. You install and configure the control point application (1) on the workstation you designate as the control point. Then, you install and configure the other components on a single, separate workstation. These components include: the control database (2), the watchdog server (3), the operating system and database drivers (4), and the watchdogs (5). These procedures are covered in detail in “Configuring a Control Database” on page 47.

If you follow this approach, it is recommended that the watchdog server reside on the same workstation as the control database; however, you can install it on the same workstation as the control point application.

Setting Up Multiple Watchdogs per Database Instance

In a distributed management environment where there are multiple control points, you might need to have more than one control point manage the same database. This option is feasible if you have database administrators who specialize in separate scopes of responsibility; or, for example, if you assign a separate control point application for the help desk.

If you choose to dedicate each control point to its own limited set of administrative functions among every database and managed host, every database watchdog associated with a particular control point would be alike—likewise for the operating system watchdogs. Each database instance and managed host would have multiple sets of watchdogs, each assigned to its particular control point (see Figure 6).

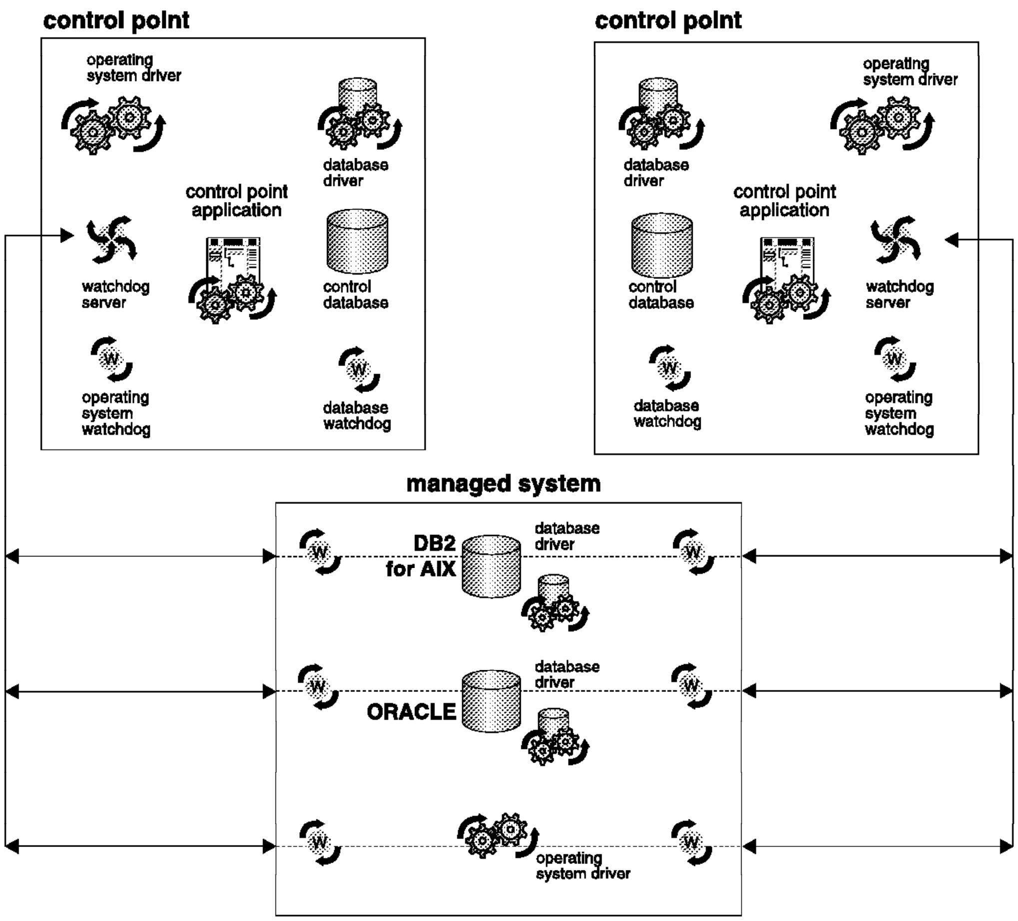

Figure 6. Sample Configuration with Multiple Watchdogs per Database Instance

Installing and configuring multiple watchdogs for each database instance requires completing a standard installation and configuration with a few additional steps. You will install and configure watchdogs (and drivers, if needed) for each database instance. You then configure another occurrence of the watchdogs, but specify a connection to the other control point.

These additional procedures are in “Configuring a Control Point Application” on page 47 and “Configuring Watchdogs” on page 51.

Planning Your DataHub Installation and Configuration

This section helps you finish your preparation for installing and configuring DataHub. It helps you understand the installation process and lists some final considerations for your environment. This section also lists hardware requirements, software requirements, and licensing considerations.

Now that you have a basic understanding of DataHub components and where they are located, you need to understand that the final DataHub configuration for your environment is set by four different activities:

Installing Copying DataHub files from the installation media to the DataHub directories on the control point and managed hosts. The installing task for each workstation must be completed prior to configuring DataHub.

Building Ing Creating DataHub INGRES components for distribution at your site. This task is specific to INGRES management by DataHub and is not required for other RDBMSs. The build task must be completed after the installing task and prior to configuring DataHub.

Configuring Setting-up the DataHub files and environment according to your specifications. Configuration sets up the control point application, loads the control database, and sets up and starts the watchdog server, drivers, and watchdogs. This task applies to the control point system and managed hosts.

DataHub provides two configuration programs: a GUI program (dhuinst) for use on systems that have OSF/Motif** 1.2 installed, and an ASCII version (dhuinstty) for other systems. While both programs provide the same capability, the GUI program is easier to use.

The examples throughout this book use the GUI program. In each case, the ASCII program can be substituted and the end result will be the same.

Migrating Preserving the DataHub files and environment while updating an existing DataHub configuration. Migration is an option available when configuring DataHub. If selected, you can make use of information in the existing control database and system files to migrate your existing DataHub release to a later level.

This process requires the dhuinst configuration program. The dhuinstty program does not support migration.

Determining Your DataHub Environment

For both typical and complex environments, you must:

1. Determine which hosts and databases you want to manage.
2. Determine if you need more than one control point.
   a. In large-scale scenarios, decide whether there is a need for distributed database systems management by multiple database administrators (DBAs). DataHub can provide system and database management from one or more control points.
   b. Determine how many administrators your single control point workstation can support. If the control point workstation can handle a high number of processes, you can choose to have multiple administrators use the same control point. You might, however, find a need to have multiple control points on separate (smaller) workstations, each managing a subset of your data network.
   c. Consider the needs of other potential DataHub users, such as help desk personnel or application developers who need to create test environments.
3. Determine which workstations will contain control points.
4. Determine whether each control point will have its own control database or share a control database with another control point.
5. Determine whether the control database resides on the same system as the control point application.

After you consider these topics, you are ready to consider the physical environment required for DataHub components.

DataHub Hardware and Software Requirements

Before you install any DataHub components, ensure that your workstation has the appropriate set of hardware and software.

Hardware Requirements

These requirements are *minimum* configuration requirements and do not allow for the simultaneous execution of DataHub and other applications.

Control Point: A DataHub control point application requires:

- A system unit that supports one of the following UNIX operating systems:

- IBM AIX Version 3.2.5, 4.1, or 4.2 for the RISC System/6000
- HP-UX Version 9.0.5 or 10.01
- Sun Solaris Operating Environment Version 2.3 or 2.4 for the Solaris SPARCstation

- A minimum of 32 MB of random access memory (RAM). Additional RAM can improve performance significantly.
- 30 MB of disk storage. An additional 25 MB is required to store the publications.
- Space in the RDBMS selected for the control database.[1]
- A supported CD-ROM reader (advisable).
- A mouse, keyboard, and display capable of supporting the X Window System and OSF/Motif.
- An Ethernet or Token-Ring network adapter (if managing other workstations).

Each Managed Host: A DataHub managed host requires:

- A system unit that supports one of the following UNIX operating systems:
  - IBM AIX Version 3.2.5, 4.1, or 4.2 for the RISC System/6000
  - HP-UX Version 9.0.5 or 10.01
  - Sun Solaris Operating Environment Version 2.3 or 2.4 for the Solaris SPARCstation
- 10 MB of RAM
- 16 MB of disk storage
- An Ethernet or Token-Ring network adapter

Software Requirements

Except where noted, the control point and each managed host require one of the following groups of software, which are listed by operating system:

- IBM AIX Version 3.2.5, 4.1, or 4.2 for the RISC System/6000 and each of the following products:
  - IBM AIXwindows Environment/6000 Version 1 Release 2.5 (control point only)

[1] For installation, the control database requires approximately 10 MB of space, depending on the RDBMS you use. During normal use of DataHub, a few database tables have the potential to grow quite rapidly; therefore, the disk partition for the control database should have space available for expansion.

- Transmission Control Protocol/Internet Protocol (TCP/IP) Version 3 Release 2 for AIX/6000

- HP-UX Version 9.0.5 or 10.01 and each of the following products:
  - OSF/Motif 1.2 and X Windows X11 Release 5 for HP-UX Version 9.0.5 or 10.01 (control point only)
  - TCP/IP for HP-UX Version 9.0.5 or 10.01

  The displayable softcopy documentation support provided for HP-UX displays an error message at startup because the support is not yet upgraded to HP-UX Version 10. Also, the Help function for the softcopy documentation display support is not available.

- Sun Solaris Operating Environment Version 2.3 or 2.4 and each of the following products:
  - OSF/Motif 1.2 and X Windows X11 Release 5 for the Sun Solaris Operating Environment 2.3 or 2.4 (control point only)
  - TCP/IP for the Sun Solaris Operating Environment Version 2.3 or 2.4

This section lists the RDBMSs supported by DataHub. At a minimum, one of the following databases, and any additional software listed with the database, is required to serve as the control database:

- IBM DATABASE 2 for AIX/6000, Version 1
- IBM DATABASE 2 for AIX, Version 2 Release 1 (or Release 1.1)
- IBM DATABASE 2 for HP-UX, Version 2 Release 1 (not supported on HP-UX 9.0.5)
- IBM DATABASE 2 for the Solaris Operating Environment, Version 2 Release 1 (not supported on Solaris 2.3)
- INGRES 6.4, including each of the following products:
  - INGRES 6.4 Q&R Tools
  - A C compiler. DataHub INGRES 6.4 support requires one of the following compilers:

    IBM AIX (Version 3.2.5)
    C Set++ for AIX Version 2.1.4

    IBM AIX (Version 4.1 or 4.2)
    C Set++ for AIX Version 3.1.3.3

    HP-UX (Version 9.0.5 or 10.01)
    HP-UX C Compiler

    Sun Solaris Operating Environment (Version 2.3 or 2.4)
    SPARCompiler C 3.0.1

- ORACLE Release 7.0, 7.1 or 7.2, including each of the following products:
  - ORACLE SQL DBA
  - ORACLE SQL Loader
  - ORACLE SQL Plus (not required for managed hosts)
- SYBASE SQL Server Release 10, 10.0.2, or 11, with the following restrictions:
  - SYBASE SQL Server (all releases) is not supported on HP-UX 10.01
  - SYBASE SQL Server Release 11 is supported only on IBM AIX Version 3.2.5, 4.1 or 4.2

Selecting a License Mode

You can run DataHub in either of two modes: temporary demonstration or licensed. Additionally, you can convert from the temporary demonstration mode to licensed mode at any time.

Temporary demonstration
Allows full but temporary usage of the DataHub product. You can use the product for 60 days, after which the product becomes unusable until it is converted to licensed mode.

This mode expires on June 30, 1997.

Licensed
Allows full use of the DataHub product. The licensed mode requires the Vendor ID and Product License Key that is included in the Product License Key label. You enter the ID and key during configuration of the control point. DataHub stores these values in the nodelock file.

Converting a Temporary Demonstration License

You can convert a license from temporary demonstration mode to licensed mode using the control point configuration programs (dhuinst or dhuinstty).

To convert a license:

1. Start the dhuinst program.
2. Select **Configure Local Installation**.
3. Select the **Convert from Demonstration to Licensed Mode** radio button.
4. Enter the Vendor ID and Product Password. Copy the Vendor ID and Product License Key from the Product License Key label included with DataHub.
5. Press **Do**.

After converting the license, select the **Cancel** push button from the DataHub control point configuration window to avoid reconfiguring DataHub.

Deciding on Your Next Step

At this point you should know what DataHub is and how you will use it.

If you know which workstations will be control points and which will be managed hosts, see Chapter 2, "Installing DataHub Control Point Files" on page 18.

If you are considering an alternative installation, even if you know which workstations will be control points and which will be managed hosts, consider browsing "Alternative DataHub Configurations" on page 8 again. Confirm that your planned configuration is consistent with the hardware and software on your workstations. After reading about alternative installations, continue with Chapter 2, "Installing DataHub Control Point Files" on page 18.

Chapter 2. Installing DataHub Control Point Files

This chapter contains the procedures for installing a DataHub control point. The instructions tell you how to move DataHub files from the distribution media to system directories on workstations.

> If you are installing DataHub as a SystemView feature, read the Installation information panel for DataHub on the SystemView CD Showcase for different installation instructions.

Before you install any DataHub components, you must determine the location for your control point, the distribution (optional—used for complex environments) of control point components, and the hosts and databases you want to manage on the control point workstation and managed host workstations. Chapter 1, "Preparing to Install and Configure DataHub" on page 1 can help you make these decisions.

This chapter starts by listing variables used for all installation tasks in "Understanding Installation Variables."

The following section ("Installing Control Point Files Using the Control Point CD-ROM Drive" on page 20) describes installation tasks for the control point.

Understanding Installation Variables

The following variables are used extensively when installing DataHub components:

> Use variable names (for path and directory variables) starting with "dh". Otherwise, all **ps** commands in this document must be modified to match the names you choose (and you will usually have to enter multiple **ps** commands to display processes.

datahub_path
The complete path name of the directory where the DataHub files are installed. An example value is /usr/sys/inst.images/dhub.

Your value is ________________________.

old_datahub_dir
: The directory where DataHub was previously installed (reinstallation only). An example value is /u/old_dhub.

Your value is ________________________.

system_dir
: One of the following system-specific directory names: AIX, HP-UX, or SunOS.

Your value is ________________________.

media_device
: The device name assigned to the install media (for example, rc0 is a common device name for a CD-ROM drive).

Your value is ________________________.

datahub_dir
: The specific directory where the DataHub files reside (the last directory in *datahub_path*). An example value is dhub.

Your value is ________________________.

managed_host_dir
: The directory where the files to be installed on a managed host are temporarily stored. An example value is /usr/sys/inst.images/dhubmh.

Your value is ________________________.

old_managed_host_dir
: The directory where the managed host files were previously installed (reinstallation only). An example value is /u/old_dhumh.

Your value is ________________________.

hostname
: The IP or DNS address of a host. An IP address example is 9.112.56.1. A DNS address example is my_workstation.enterprise.com. You can use short names, such as diamond.

Your value is ________________________.

archive_file
: The archived tar file that is copied from the CD-ROM onto your system. An example value is sun.tar.

Your value is ________________________.

Installing Control Point Files Using the Control Point CD-ROM Drive

Typically, you will install control point files on one workstation.

If you intend to distribute DataHub control point components across two or more workstations (for example, using a database on another workstation for your control database), the steps in this section must be repeated for every workstation that has one or more control point components.

When you finish this section, all control point files are copied from the installation media to the workstation.

To install control point files:

1 From the control point workstation, log in as root.

> If you are re-installing or migrating a DataHub release, stop all DataHub processes:
>
> **ps -ef | grep** dh
> **kill -9** *PID*
>
> where *PID* is the process number returned from the **ps** command. Repeat the **kill** command for each process listed.
>
> Additionally, if you are migrating a DataHub release, you must install the new DataHub release files into the existing DataHub directory.

2 Enter **df** on the command line. Ensure that you have either 15 MB (for AIX smit/installp installations) or 30 MB (all other methods) of space available in the file system that will contain DataHub files (*datahub_path*).

This total does not include the online publications. If you want to install the publications, you will need an additional 25 MB of space.

3 Insert the DataHub CD into a CD-ROM drive and mount it to the file system.

For assistance with this procedure, refer to the documentation for your particular operating system.

4 AIX only: Optional:

If you want to use smit and installp to install DataHub files on the AIX operating system, follow this step. If you would prefer to create the DataHub directories with system commands and then use the **tar** command to install DataHub files, skip to step 5 on page 21.

a Enter **smit**.

b Go through the smit installation panel selections until you reach the Install Software Products at Latest Available Level window.

c Use the **List** option and select **1.2.0.0 dhu** as the product to install.

The files are placed in the directory /usr/lpp/dhu. The workstation now has all the files you need to configure a control point.

d Read the README.DHU file in the readme directory. It contains last-minute changes that can affect DataHub installation and configuration procedures.

e Proceed to one of the following topics:

- DB2v1 DB2v2 Ora Syb control databases: "Preparing to Configure a Control Point" on page 26
- Ing control databases: Chapter 3, "Building DataHub INGRES Components" on page 23

Do either step 4 on page 20 or steps 5 through 9 on page 22. Do not do both.

5 Create a directory for DataHub. Throughout the rest of the procedure, this directory is referred to as *datahub_path*. The following examples use the system default *user directory* as the location for the DataHub directory, but you can create the DataHub directory anywhere you want.

Enter one of the following commands to create the directory:

AIX	**cd** /u **mkdir** *datahub_dir*
HP	**cd** /usr **mkdir** *datahub_dir*
Sun	**cd** /opt **mkdir** *datahub_dir*

6 Make *datahub_path* the current directory:

cd *datahub_dir*

7 Copy the appropriate installation files to the current directory:

AIX	**tar -xvf** /dev/*media_device*/aix.tar
HP	**tar -xvf** /dev/rmt/*media_device*/hp.tar

Sun	**tar -xvf** /dev/rmt/*media_device*/sun.tar

Your workstation now has all the files you need to configure the control point.

8 Read the README.DHU file in the readme directory. It contains last-minute changes that can affect DataHub installation and configuration procedures.

9 Proceed to one of the following topics:

- DB2v1 DB2v2 Ora Syb control databases: "Preparing to Configure a Control Point" on page 26
- Ing control databases: Chapter 3, "Building DataHub INGRES Components" on page 23

Chapter 3. Building DataHub INGRES Components

If you want DataHub to manage INGRES databases or use an INGRES database for the control database, you must build DataHub INGRES components.

The build procedure requires several DataHub files. You must install DataHub control point or managed host files before attempting a build. The build procedure also requires a C compiler and local access to INGRES files. These requirements are listed in "Software Requirements" on page 14.

The files created by this procedure are platform-specific; therefore, at a minimum, you must complete this procedure once for each operating system type (AIX 3.2.5, AIX 4.1, HP-UX, and Sun Solaris) containing INGRES databases you intend to manage.

There are two approaches to using the build procedure:

- Execute the build script every time you finish installing control point or managed host files on a workstation.
- Execute the build script one time per operating system type, and then copy the build results (files) to other workstations containing DataHub (previously installed). This approach reduces build time; however, you must copy the built files from one workstation to another.

The following procedure applies to both approaches. To build INGRES files:

1. Log in to the control point host or managed host as root.
2. Change to the directory containing the driver build script:

   cd *datahub_path*/*system_dir*/drivers/ing64/obj
3. Run the build script:

   build_ing_drv

   After a few minutes, you will see the message:

   Build complete. Driver file is ready.
4. Change to the directory containing the watchdog build script:

   cd *datahub_path*/*system_dir*/watchdog/ing64/obj
5. Run the build script:

   build_ing_wdog

   After a few minutes, you will see the message:

Build complete. Watchdog file is ready.

You now have the required files for DataHub INGRES operations on workstations using the same operating system as the current workstation.

6 Copy the files to each managed host or control point that will manage INGRES databases:

a Login to the workstation requiring DataHub INGRES files as root:

telnet *hostname*

b Change to the directory containing DataHub driver files on the target workstation:

cd *datahub_path*/*system_dir*/drivers

c Use the **ftp** command to log in to the source workstation (as root). A prompt similar to ftp> appears.

d Change to the directory containing DataHub driver files on the source workstation:

ftp> **cd** *datahub_path*/*system_dir*/drivers

e Set the file transfer mode to binary:

ftp> **binary**

f Copy one file to the target workstation:

ftp> **get** ing64d

g Change the target workstation directory to the directory containing the DataHub watchdog files:

ftp> **lcd** *datahub_path*/*system_dir*/watchdog

h Change the source workstation directory to the directory containing the DataHub INGRES watchdog file:

ftp> **cd** *datahub_path*/*system_dir*/watchdog

i Copy one file to the target workstation:

ftp> **get** watchdog.ing64

j Quit the ftp session:

quit

k Change permissions on the new files:

chmod 755 watchdog.ing64
cd *datahub_path*/*system_dir*/drivers
chmod 755 ing64d

l End the telnet session:

exit

m For each workstation of the same operating system type requiring INGRES files, repeat steps 6a on page 24 through 6m.

Continue with Chapter 4, “Configuring a DataHub Control Point” on page 26 (you should configure a control point before configuring a managed host) or Chapter 7, “Configuring a DataHub Managed Host” on page 59.

Chapter 4. Configuring a DataHub Control Point

You must configure a DataHub control point before using the product. While configuring DataHub, you can choose to migrate DataHub components from a previous release.

For all configuration activities on all workstations, you will use one of two programs: dhuinst or dhuinstty. The dhuinst program provides a graphical interface. The dhuinstty program is a text-only program that provides equivalent function without requiring OSF/Motif.

> If you are installing and configuring DataHub as a SystemView feature:
>
> - Use the dhuinst.sva program instead of the dhuinst or dhuinstty programs.
> - Read the Installation information panel for DataHub on the SystemView CD Showcase CD-ROM before configuring DataHub.

The instructions in this chapter refer to dhuinst.

Preparing to Configure a Control Point

This section lists steps you need to do before configuring a DataHub control point.

1 Create (or determine) the DataHub control database. This database must exist before the configuration program starts. If you are migrating a current DataHub configuration, you do not need to create a new database (you must use your current control database to migrate a DataHub configuration).

To create a new control database:

a Determine the control database location:

DB2v1 and DB2v2	The instance name
Ing	The INGRES RDBMS installation directory name (the value of II_SYSTEM)
Ora	The directory name (the value of the ORACLE_HOME environment variable)
Syb	The directory name (the value of the SYBASE environment variable)

b Syb only: Determine both:

- The name of the Sybase server to hold the control database.
- The Sybase server login name and password used to access Sybase. This Sybase login must have access to all managed databases, including the master database. The level of authority required is dependent on the watchdog checks. Typically, the level is an SA role. The login is used by the watchdog server and by the Sybase database watchdog.

c Create the control database.

For more information on this step, refer to the documentation provided with your RDBMS. Ensure that your database is created using the appropriate code page for your environment.

2 Start a shell session as root:

su root

3 Add an entry to the file /etc/inittab to start the RDBMS automatically on startup. The RDBMS used for the control database must be started before the DataHub background processes are started (the configuration procedure adds the startup script names for the DataHub background processes to /etc/inittab). Refer to your system and database manuals for the exact procedure. The following example shows an ORACLE startup entry:

```
oradb:2:wait:/bin/su oracle -c\
/db1/dba/oracle/product/7.0.16/bin/dbstart
```

4 Create user IDs.

a Create the user ID to use to populate the tables in the DataHub control database. This user ID is the only one that can initially access DataHub.

DB2v1 and DB2v2	The owner of the DataHub control tables and views. This ID must have DBADM authority.
Ing	The user ID that created the database (database owner).
Ora	The owner of the DataHub control tables and views. This ID must have DBA authority. Additionally, this user must not be an ORACLE externally identified user ID.

Syb	The Sybase server login name that owns the DataHub control tables and views.

b Create the database watchdog user ID:

DB2v1 and DB2v2	A database user ID that has SYSADM authority.
Ora	A database user ID that is externally identified. This ID must have authority (typically, DBA level) to perform watchdog checks.
Ing	An INGRES user ID, defined using the accessdb utility, that has the authority to perform watchdog checks. This user should have DBA authority.
Syb	This ID is the user ID that the watchdog process for Sybase runs under (the ID that started the process). This user ID can be an ordinary UNIX user ID.

5 Ensure that you have TCP/IP connectivity.

6 Check your umask setting; it can affect the installation of DataHub. For example, a umask of 027 causes some of the files built by the installation procedure to have the wrong permissions. Most DataHub files require permissions of 755; therefore, the maximum umask setting is 022. To see your current umask setting, type **umask**.

7 Optional: Collect DataHub configuration printer information.

8 Optional: Modify the X resource definitions of dhuinst.

X resources specify to the X Window System the settings for colors, fonts, the window position, and other attributes.

If you want to modify these resources, add symbolic links to the installation program's X resource definitions:

AIX	**cd** /usr/lib/X11/app-defaults **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn **ln -s** *datahub_path*/AIX/startup/XDhuInstall XDhuInstall **ln -s** *datahub_path*/AIX/startup/XStatus XStatus **ln -s** *datahub_path*/AIX/startup/XWarn XWarn
HP	**cd** /usr/lib/X11/app-defaults **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn **ln -s** *datahub_path*/HP-UX/startup/XDhuInstall XDhuInstall **ln -s** *datahub_path*/HP-UX/startup/XStatus XStatus **ln -s** *datahub_path*/HP-UX/startup/XWarn XWarn
Sun	**cd** /opt/SUNWmotif/lib/app-defaults **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn **ln -s** *datahub_path*/SunOS/startup/XDhuInstall XDhuInstall **ln -s** *datahub_path*/SunOS/startup/XStatus XStatus **ln -s** *datahub_path*/SunOS/startup/XWarn XWarn

9 Optional: Change the owner and group of the DataHub directories and executables from a default value of root:sys to another user ID and group. The following example changes owner and group to bin:

chown -R bin:bin *datahub_path*

You are now ready to begin configuring a control point.

Configuring a Control Point

The procedure in this section guides you through the steps for configuring a DataHub control point with all control point components on a single workstation.

There are three tasks associated with configuring a control point: starting and using the dhuinst program, checking your results, and starting DataHub. Appendix A, "DataHub System Modifications" on page 96 lists the modifications dhuinst makes to your system.

To start the dhuinst program:

1 Log in to the control point workstation.

2 If you want to migrate a current DataHub release, back up your current control database.

> When you migrate a DataHub release, the current control database is overwritten. Back up the current control database before starting the configuration program.

3 Switch user to root:

su root

4 Set the locale to a valid language (other than C or POSIX) so the control database is populated using the correct code page.

AIX	**export** LANG=En_US
HP	**export** LANG=english
Sun	**export** LANG=en

You can enter the **locale -a** command to determine which languages are installed on your workstation.

5 Set the NLS path.

The following statement (in Korn shell syntax) can be used to set the path:

export NLSPATH=$NLSPATH:*datahub_path/system_dir/*msg/%L/%N:\
*datahub_path/system_dir/*msg/C/%N

An example statement is:

export NLSPATH=$NLSPATH:/usr/lpp/dhu/AIX/msg/%L/%N:\
/usr/lpp/dhu/AIX/msg/C/%N

6 If you are configuring DataHub with LANG=Ja_JP or LANG=zh_CN and you started X Windows using some other setting, modify the DataHub configuration resource files (XDhuInstall, XStatus and XWarn):

a Enter: **cd** *datahub_dir/system_dir/*startup

b For Japanese, edit the resource files and add the following line:

*fontList : *-gothic-*:

c For Simplified Chinese, edit the resource files and add the following line:

*fontList : *-song-*:

d Set up your system to use these resource files. Do one of the following steps:

- Copy the resource files to root's home directory.
- Add a symbolic link from the app-defaults directory to the resource files. See step 8 on page 28.
- Set (and export) XAPPLRESDIR to the DataHub startup directory using the following command:

  export XAPPLRESDIR=*datahub_dir/system_dir/*startup

7 Start the configuration program:

cd *datahub_path/system_dir/*install
./**dhuinst**

A window appears (Figure 7).

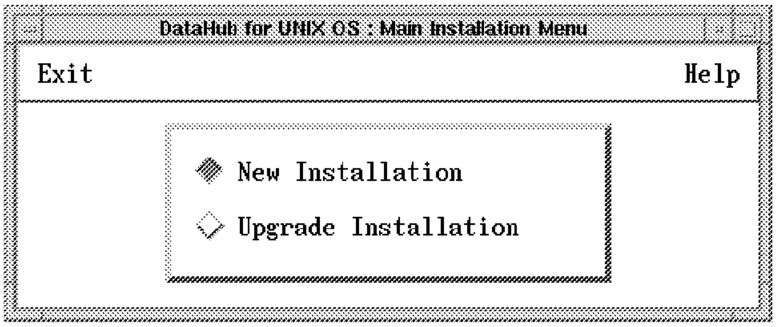

Figure 7. DataHub Main Installation Window

At this point, you must decide if you are migrating your existing DataHub control point to a newer release of DataHub or configuring a new control point.

If a control point configuration does not currently exist on this workstation, you must select the first option (**New Installation**). You can also use this option to replace an existing control point configuration.

The migration procedure (**Upgrade Installation**) re-uses configuration data currently located in your control database and system files. Migrating data will simplify your configuration process (the program finds values on your system instead of waiting for your input) and preserve many aspects of your current DataHub environment. Current watchdog server, watchdog, and driver information is retained. Substantial portions of your current control database are preserved.

Migration is supported only from DataHub Release 1.1 to DataHub Release 2.

Do one of the following steps:

a To configure a new control point or replace an existing control point configuration, select the **New Installation** radio button.

Continue with "Configuring a New DataHub Control Point."

b To migrate your current DataHub release, select the **Upgrade Installation** radio button.

Continue with "Migrating a DataHub Control Point" on page 37.

Configuring a New DataHub Control Point

This section contains the configuration procedure steps you follow after starting the dhuinst program and selecting the **New Installation** radio button in the first window.

To configure a new DataHub control point:

1 Select the **Configure Local Installation** button.

The Configure Local Installation window appears (see Figure 8 on page 33).

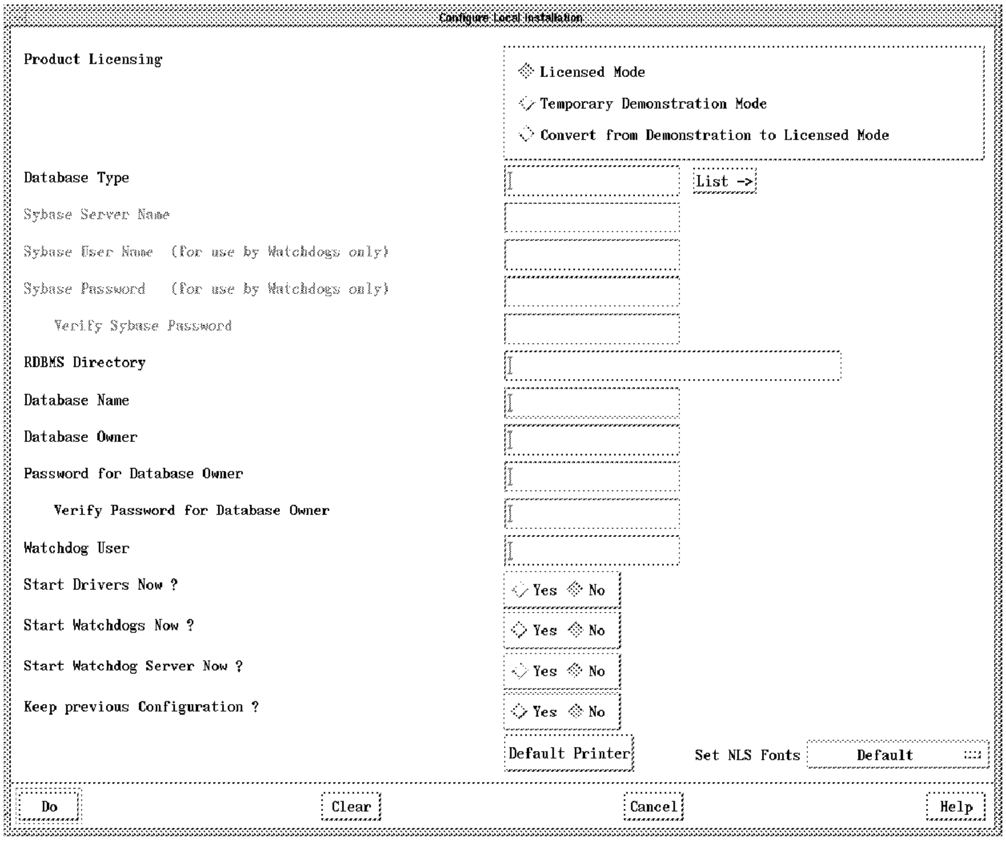

Figure 8. Configure Local Installation Window

2 Fill in the fields. Table 2 on page 34 describes the information required for each field. Certain fields are database dependent and appear only when their associated database type is selected. Refer to the online help for details.

To open help for the window task, select the **Help** push button. To obtain help for a particular field, select the field and press F1.

Table 2 (Page 1 of 2). Fields in the Configure Local Configuration Window	
Field	***Action***
Product Licensing	Select the appropriate mode: • **Licensed Mode** installs DataHub using a nodelock license. • **Temporary Demonstration Mode** installs DataHub using a 60 day trial license. • **Convert from Demonstration to Licensed Mode** converts the trial license to a node-lock license.
Database Type	Select the **List ->** push button and select the type of database you want to use as the control database.
Sybase Server Name	Syb Type the Sybase server name.
Sybase User Name (for use by Watchdogs only)	Syb Type the Sybase server login name to be used to access Sybase. This Sybase login should have access to all managed databases, including the master database. The level of authority required is dependent on the watchdog checks. Typically, the level is an SA role. The login is used by the watchdog server and by the Sybase database watchdog.
Sybase Password	Syb Type the password for the above login name.
Verify Sybase Pass-word	Syb Retype the login name password.
RDBMS Directory	Ing Type the directory corresponding to the II_SYSTEM environment variable for the INGRES RDBMS containing the control database. Ora Type the directory location of the data-base to contain the control database tables (the directory location should match the value of the ORACLE_HOME environment variable). Syb Type the directory where the Sybase server is located (the directory location should match the value of the SYBASE environment variable).
Database Instance Name	DB2 Type the name of the database instance for the control database.
Database Name	Type the name of the database where the DataHub control database tables are to be stored.

Table 2 (Page 2 of 2). Fields in the Configure Local Configuration Window	
Field	***Action***
Database Owner	DB2 Ora Ing Type the user ID of the owner of the DataHub control database tables. This ID is also used by the watchdog server to access the control database. Syb Type the Sybase server login name for the configuration procedure to use to populate the control database tables.
Password for the Database Owner	Type the database owner's password.
Verify Password for Database Owner	Retype the password for verification.
Watchdog User	Type the user ID to be used by the database watchdog: DB2v1 Type a database user ID that has SYSADM authority. DB2v2 Type a database user ID that has SYSADM authority. In the instance owner's default environment, the variables user and db2instance must be set to the instance name. Ing Type a database user ID, defined using the accessdb utility, that has the authority to perform watchdog checks. This user should have DBA authority. Ora Type a database user ID that is externally identified. This ID must have authority to perform watchdog checks. Syb Type a user ID. This ID is the user ID that the watchdog process for Sybase runs under (the ID that started the process). This user ID can be an ordinary UNIX user ID.

3 Select the **Yes** radio button for each of the following fields:

Start Drivers Now ?
Start Watchdogs Now ?
Start watchdog server Now ?

Selecting these options starts the script files (rc.dhudrv, rc.dhu_gcs, rc.dhu_sms, rc.dhu_ia, rc.dhuwdg) that activate the DataHub *daemon* processes.

4 Select the **No** radio button for the **Keep Previous Configuration ?** field.

Selecting this option replaces any drivers and watchdogs installed by a previous release of DataHub.

5 Optional: To have the configuration procedure set up a default printer:

a Select the **Default Printer** push button. The Configure Default Printer window appears.

b Fill in the fields of the Configure Default Printer window and select the **Do** push button.

For instructions on how to manually set or change the default printer settings, see “Defining a PostScript Printer” on page 71.

6 Specify the correct national language font list. Select the **Set NLS Fonts** push button. The choices are:

- **Default** (all available languages except Japanese and Simplified Chinese)
- **Japanese**
- **Chinese**

7 Select the **Do** push button. The configuration program starts making changes to your system. The procedure takes from 3 to 15 minutes, depending on your system.

> If DataHub was previously installed, several windows appear asking if you want to continue or replace various soft links.
>
> In general, you should choose to replace the links; however, if you have already installed IPF/X for use by another application, there may be an existing link to the libipfx.a file. By changing this link (and possibly removing it), you could cause the other application's help to stop running. Also, if a patch for IPF/X is installed (later) for the other application, changing the link can prevent the application from running with the latest IPF/X patch.

8 If you require more database drivers or watchdogs, see the instructions in “Configuring Drivers” on page 49 and “Configuring Watchdogs” on page 51. You will need additional watchdogs, and possibly additional drivers, if you want to manage two or more databases on the control point workstation.

Continue with “Checking Control Point Configuration Results” on page 40 (skip “Migrating a DataHub Control Point” on page 37).

Migrating a DataHub Control Point

This section contains the configuration procedure steps you follow after starting the dhuinst program and selecting the **Upgrade Installation** radio button in the first window.

Before you migrate your control point, read “Migration Considerations.” If the migration procedure restrictions are acceptable, continue the migration procedure with “Migration Steps.” If the restrictions are not acceptable, exit back to the Main Configuration window, select the **New Installation** button, and continue with “Configuring a New DataHub Control Point” on page 32.

Migration Considerations

The DataHub migration process preserves the following information:

- Managed host definitions
- Managed database definitions
- Managed Sybase server definitions
- DataHub groups, users, and their privileges
- User defined objects and actions
- Configured watchdog checks and rules
- Configured driver and watchdog types
- Configured printers

We recommend that you migrate DataHub components.

The migration procedure, however, does not preserve 100% of an existing configuration. Restrictions include:

- Resource file settings (colors and fonts) are not migrated.
- Any checks you have placed in DBA_PRED_CHECKS are not migrated.
- You must use the dhuinst (not dhuinstty) program to migrate DataHub configurations.

Migration Steps

At this moment you should see Figure 9 on page 38.

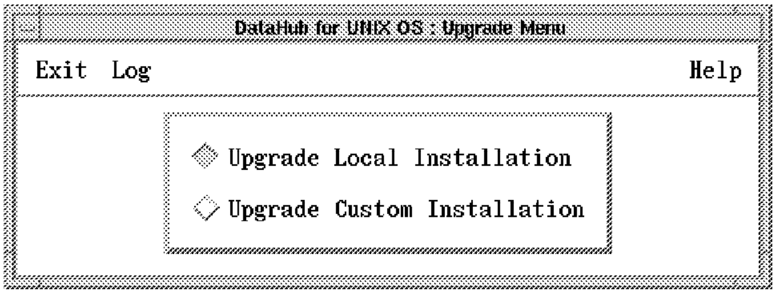

Figure 9. Upgrade Local or Custom Installation Window

To migrate a DataHub control point:

1 Select the **Upgrade Local Installation** button.

The Upgrade Local Installation window appears (see Figure 10).

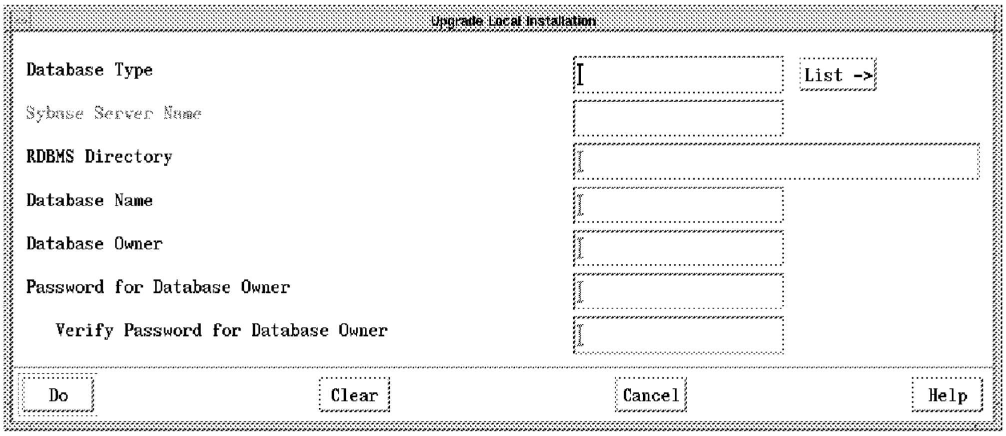

Figure 10. Upgrade Local Installation Window

2 Fill in the fields. Table 3 on page 39 describes the information required for each field. Certain fields are database dependent and appear only when their associated database type is selected. Refer to the online help for details.

To open help for the window task, select the **Help** push button. To obtain help for a particular field, select the field and press F1.

Table 3. Fields in the Upgrade Local Configuration Window	
Field	***Action***
Database Type	Select the **List ->** push button and select the type of database currently used as the control database (you cannot change the database type during migration).
Sybase Server Name	Syb Type the Sybase server name used by the current control database
RDBMS Directory	Ora Type the directory location of the database to contain the control database tables (the directory location should match the value of the ORACLE_HOME environment variable). Syb Type the directory where the Sybase server is located (the directory location should match the value of the SYBASE environment variable).
Database Instance Name	DB2 Type the name of the database instance for the control database.
Database Name	Type the name of the database where the DataHub control database tables are to be stored. This value must match the current control database name.
Database Owner	Type the database owner name. DB2 Ora Type the current user ID of the owner of the DataHub control database tables. Syb Type the Sybase server login name for the configuration procedure to use to populate the control database tables.
Password for Database Owner	Type the database owner's password.
Verify Password for Database Owner	Retype the database owner's password for verification.

3 Select the **Do** push button. The migration program starts making changes to your system. The procedure takes from 3 to 15 minutes, depending on your system.

Several windows appear asking if you want to continue or replace various soft links.

In general, you should choose to replace the links; however, if you have already installed IPF/X for use by another application, there may be an existing link to the libipfx.a file. By changing this link (and possibly removing it), you could cause the other application's help to stop running. Also, if a patch for IPF/X is installed (later) for the other application, changing the link can prevent the application from running with the latest IPF/X patch.

Continue with "Checking Control Point Configuration Results."

Checking Control Point Configuration Results

To check your results:

1 Check the install log to make sure the operation was successful. You can do this from within the configuration program by selecting the **View Log File** option from the **Log** menu of either the Configuration Menu (new configuration) window or the Upgrade Menu (migration) window.

You can check the install log at any time after the configuration is finished. One method of viewing the file is:

cat *datahub_path*/*system_dir*/install/install.log **| pg**

You might want to make a copy of this log file, because it is overwritten each time the configuration program is started.

The install log contains the password used for the Sybase server; therefore, use discretion if you reference this file. Two other files generated by the installation program, general.mem and local.mem, also contain password information and should be protected. For more information, see Appendix C, "DataHub Passwords" on page 100.

2 Quit the root command shell:

exit

3 Set the locale (examples given in Korn shell syntax):

export LANG=*language_id*

where *language_id* is:

AIX	En_US Ja_JP zh_CN

HP	english
Sun	En

4 Make the **datahub** command accessible. You have two options; the first is recommended:

- Set a symbolic link in a directory already in the system standard path:

  cd /usr/bin
  ln -s *datahub_path*/*system_dir*/gui/datahub datahub

- Include *datahub_path* in the system path.

  export PATH=*datahub_path*/*system_dir*/gui:$PATH

In both options, *datahub_path* refers to the *full* path name, beginning with the root directory, /.

5 Optional: Add the **export** statement in step 3 on page 40 to the startup file for each DataHub user (for example, the user's ~/.profile file for Korn shell users).

6 Start DataHub, using one of the following steps:

- If a DataHub (datahub) link was established, enter:

  datahub

- If a link was not established:

  cd /*datahub_path*/*system_dir*/gui
  ./datahub

The Login window appears.

7 Log in with the user ID and password of the control database owner; at this point, this user ID is the only one with access to DataHub (for information on authorizing users access to DataHub, refer to the *DataHub for UNIX Operating Systems User's Guide*).

After DataHub reads the control database information, the main window appears. The local host object occurrence appears under the host object type in the Object Tree window (see Figure 11). If it does not appear, or if you experience any problems, refer to Chapter 9, "Troubleshooting DataHub Conditions and Messages" on page 78.

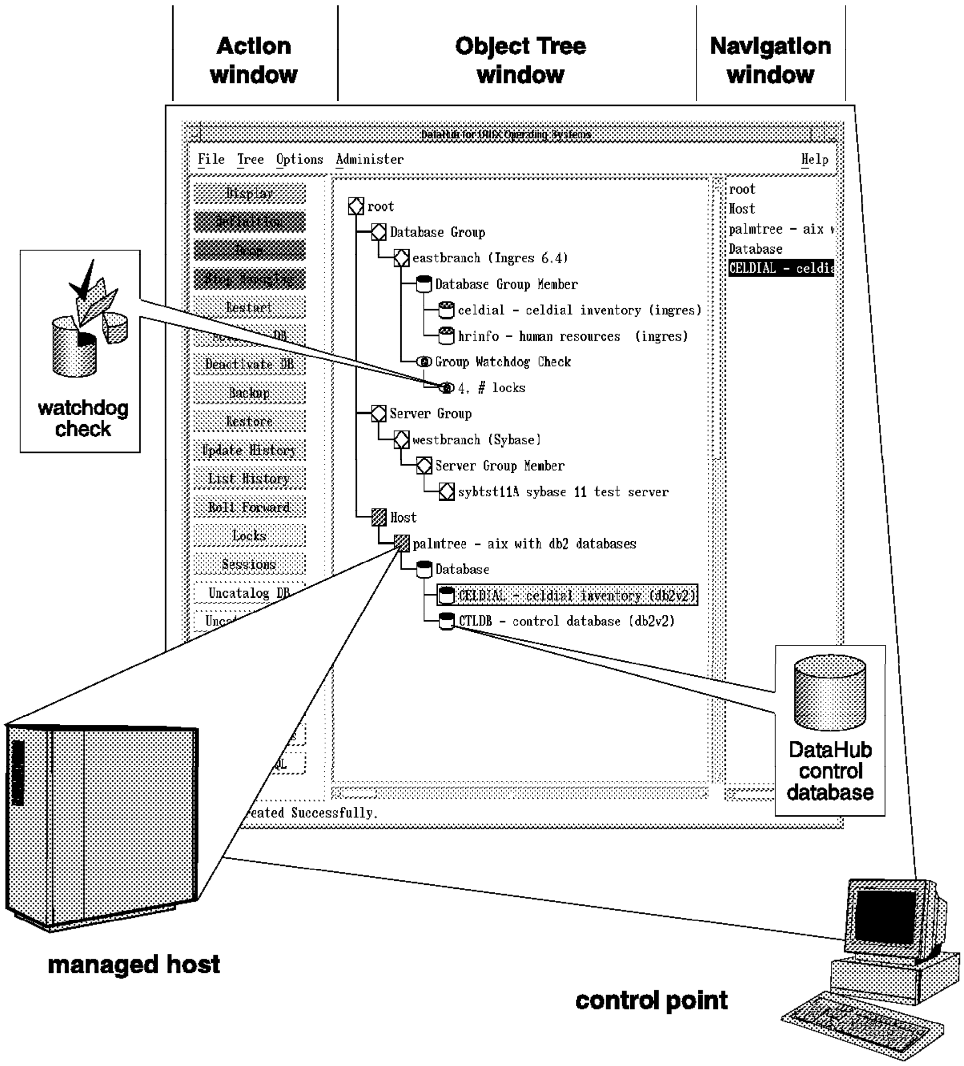

Figure 11. DataHub for UNIX Operating Systems Main Window

Chapter 5. Configuring DataHub Components: Alternative Options

This chapter is provided for users requiring an alternative DataHub configuration. If the standard configuration documented in "Configuring a Control Point" on page 29 is sufficient for your business needs, skip this chapter.

Each procedure in this section configures a specific control point or managed host component of DataHub. Use these procedures if you want to configure your system in a way similar to any of the sample control point configurations mentioned in "Alternative DataHub Configurations" on page 8 or if you have an environment requiring a customized arrangement of DataHub components.

To complete the following procedures, use the dhuinst or dhuinstty configuration programs. The configuration programs must be run from the workstation on which the component you want to configure resides.

If you haven't previously installed any DataHub components on this workstation, refer to one of these procedures:

- To install a control point component, complete the procedures in "Installing Control Point Files Using the Control Point CD-ROM Drive" on page 20.
- To install managed host components, complete the procedures in either "Installing Managed Host Files Using the Managed Host CD-ROM Drive" on page 53 or "Installing Managed Host Files Using the Control Point CD-ROM Drive" on page 55.

Prepare for your configuration of DataHub components. Refer to one of these procedures:

- If you will configure a control database, do the steps in "Preparing to Configure a Control Point" on page 26 before starting the configuration program.
- If you will configure a control point, do the steps in "Preparing to Configure a Control Point" on page 26 (skip steps 1 on page 26, 3 on page 27, and 4a on page 27) before starting the configuration program.
- For all other components, do the steps in "Preparing to Configure a Managed Host Component" on page 59 before starting the configuration program.

If you want to migrate a current DataHub release, back up your current control database.

When you migrate a DataHub release, the current control database is overwritten. Back up the current control database before starting the configuration program.

You begin each of the procedures in this section by starting the configuration program:

1 Log in as root.

2 Set the locale to a valid language (other than C or POSIX) so that the control database will be populated using the correct code page. For example:

export LANG=En_US

You can enter the **locale -a** command to determine which languages are installed on your workstation.

3 Set the NLS path.

The following statement (in Korn shell syntax) can be used to set the path:

export NLSPATH=$NLSPATH:*datahub_path/system_dir/*msg/%L/%N:\
*datahub_path/system_dir/*msg/C/%N

An example statement is:

export NLSPATH=$NLSPATH:/usr/lpp/dhu/AIX/msg/%L/%N:\
/usr/lpp/dhu/AIX/msg/C/%N

4 If you are configuring DataHub with LANG=Ja_JP or LANG=zh_CN and you started X Windows using some other setting, modify the DataHub configuration resource files (XDhuInstall, XStatus and XWarn):

a Enter: **cd** *datahub_dir/system_dir/*startup

b For Japanese, edit the resource files and add the following line:

*fontList : *-gothic-*:

c For Simplified Chinese, edit the resource files and add the following line:

*fontList : *-song-*:

d Set up your system to use these resource files. Do one of the following steps:

- Copy the resource files to root's home directory.
- Add a symbolic link from the app-defaults directory to the resource files. See step 4 on page 60.

- Set (and export) XAPPLRESDIR to the DataHub startup directory using the following command:

  export XAPPLRESDIR=*datahub_dir/system_dir/*startup

5 Start the configuration program:

cd *datahub_path/system_dir/*install
./**dhuinst**

A window appears (Figure 12).

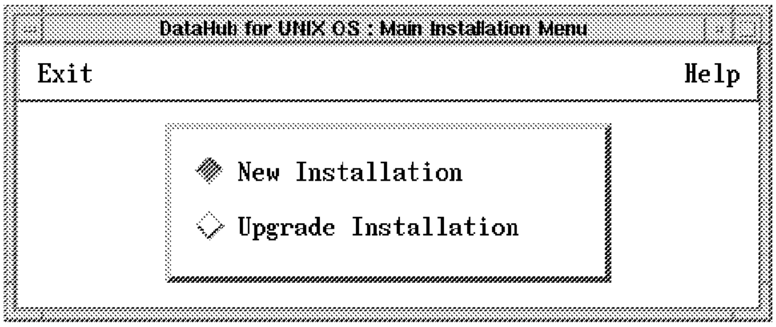

Figure 12. DataHub Main Installation Window

At this point, you must decide if you are migrating your existing DataHub configuration to a newer release of DataHub or configuring new components.

If a control point or other DataHub component configuration does not currently exist on this workstation, you must select the first option (**New Installation**). You can also use this option to replace an existing configuration.

The migration procedure (**Upgrade Installation**) re-uses configuration data currently located in your control database and system files. Migrating data will simplify your configuration process (the program finds values on your system instead of waiting for your input) and preserve many aspects of your current DataHub environment. Current watchdog server, watchdog, and driver information is retained. Substantial portions of your current control database are preserved.

> Migration is supported only from DataHub Release 1.1 to DataHub Release 2.
>
> For more information, refer to "Migration Considerations" on page 37.

Do one of the following steps:

a To configure a new control point (or other DataHub component) or replace an existing control point configuration, select the **New Installation** radio button.

Select the **Configure Custom Installation** radio button. A new window opens.

Continue with the specific instructions (starting with step 2) in one of the following sections:

- "Configuring a Control Point Application" on page 47
- "Configuring a Control Database" on page 47
- "Configuring a Watchdog Server" on page 49
- "Configuring Watchdogs" on page 51
- "Configuring Drivers" on page 49

b To migrate current DataHub components, select the **Upgrade Installation** radio button.

Select the **Upgrade Custom Installation** radio button. A new window opens (Figure 13).

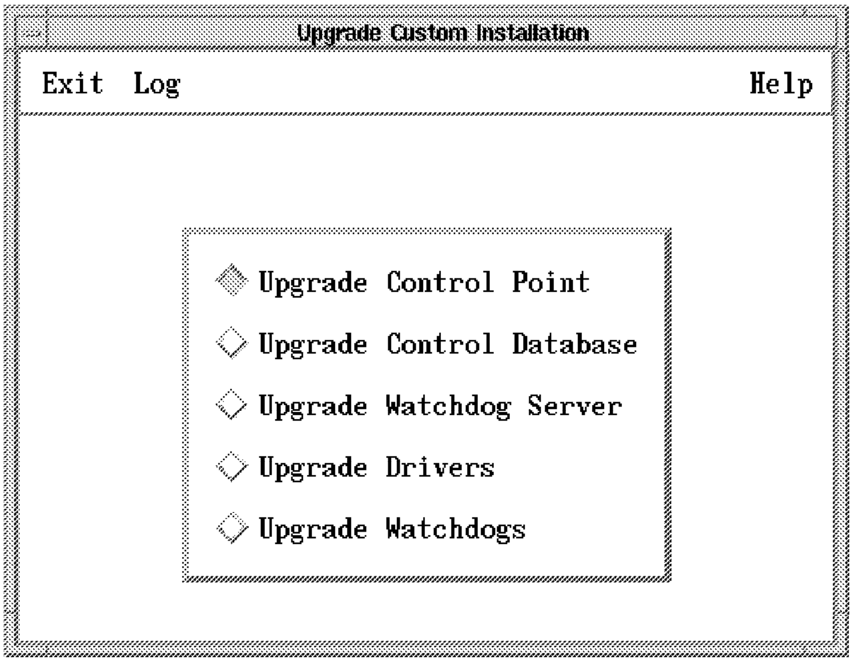

Figure 13. Upgrade Custom Installation Window

For all selections, except **Upgrade Control Database**, the only required step is selecting an option. The selected components are then upgraded without additional screens or input.

Upgrade a component at this time by selecting an option.

If you are upgrading a control database, continue with step 2 in “Migrating a Control Database” on page 48.

Configuring a Control Point Application

In a typical DataHub environment, the control point application and the control database are on the same system. However, it is possible to have the control point application and the control database on separate systems, or to have multiple control point applications on different workstations share a single control database.

To configure a control point application:

1. Perform the steps in Chapter 5, “Configuring DataHub Components: Alternative Options” on page 43.
2. Select the **Configure Control Point** radio button. A new window opens.
3. Fill in the window fields as appropriate. If you need assistance, open the online help by selecting or tabbing to a field and pressing F1. Alternatively, read the window explanations in Table 2 on page 34.
4. Optional: To automatically set up a default printer, select the **Default Printer** push button.
5. Select the correct national language font list. Select the **Set NLS Fonts** push button. The selections are:
   - **Default** (all available languages except Japanese and Simplified Chinese)
   - **Japanese**
   - **Chinese**
6. Select the **Do** push button. The configuration process starts.

You have configured your control point application. To check your results and prepare DataHub for use, see “Checking Control Point Configuration Results” on page 40.

Configuring a Control Database

In a typical DataHub environment, the control database and the control point application are on the same system; however, it is possible to have the control database and the control point application on separate systems. These procedures configure or migrate the DataHub control database for either case.

When following these procedures, you must be logged in to the workstation where the control database will be located (or is currently located). Configuration and migration procedures require that the control database exist before starting the dhuinst program.

Continue with either “Configuring a New Control Database” or “Migrating a Control Database.”

Configuring a New Control Database

Before starting the configuration procedures, create or select a database that will become your control database.

To configure a DataHub control database:

1. Perform the steps in Chapter 5, “Configuring DataHub Components: Alternative Options” on page 43. In the last step (5 on page 45), select the **New Installation** radio button.
2. Select the **Configure Control Database** radio button. A new window opens.
3. Fill in the window fields as appropriate. If you need assistance, open the online help by selecting or tabbing to a field and pressing F1.
4. Select the **Do** push button. The configuration process starts.

The new control database is ready.

Migrating a Control Database

To migrate a DataHub control database:

1. Perform the steps in Chapter 5, “Configuring DataHub Components: Alternative Options” on page 43. In the last step (5 on page 45), select the **Upgrade Installation** radio button.
2. Fill in the window fields as appropriate. If you need assistance, open the online help by selecting or tabbing to a field and pressing F1.
3. Select the **Do** push button. The configuration process starts.

The migrated control database is ready.

Configuring a Watchdog Server

In a typical DataHub environment, the watchdog server is located on the same workstation as the control point application and the control database. However, it is possible to have the watchdog server on a different workstation.

To configure a DataHub watchdog server:

1 Perform the steps in Chapter 5, "Configuring DataHub Components: Alternative Options" on page 43.

2 If creating a new watchdog server (migrating a watchdog server requires only the steps in Chapter 5, "Configuring DataHub Components: Alternative Options" on page 43), select the **Configure Watchdog Server** radio button. A new window opens.

3 Fill in the window fields as appropriate. If you need assistance, open the online help by selecting or tabbing to a field and pressing F1. Alternatively, read the window explanations in Table 2 on page 34.

If you want to start the watchdog server now, select the **Yes** radio button. If you want to start it at a later time, select the **No** radio button.

4 Select the **Do** push button. The configuration process starts.

The new watchdog server is now ready. If you experience any problems with the watchdog server, see "Checking Common DataHub Processes" on page 78.

> If you selected the **No** option for starting the watchdog server, you can start it now (manually) by entering (in this exact order):
>
> **/etc/rc.dhu_gcs**
> **/etc/rc.dhu_sms**
> **/etc/rc.dhu_ia**

Configuring Drivers

DataHub can manage multiple databases on the control point or on managed hosts. The following procedure can configure the control database driver, add additional drivers to the control point, or add drivers to a managed host.

If you adding additional drivers to an existing DataHub workstation, make sure that the DataHub driver processes are not running. For more information, see “Checking Common DataHub Processes” on page 78.

You might need to follow the steps in this section several times.

To configure DataHub drivers:

1 Perform the steps in Chapter 5, “Configuring DataHub Components: Alternative Options” on page 43.

2 If you are creating new drivers (migrating drivers requires only the steps in Chapter 5, “Configuring DataHub Components: Alternative Options” on page 43), select the **Configure Drivers** radio button. A new window opens.

3 Fill in the window fields as appropriate. If you need assistance, open the online help by selecting or tabbing to a field and pressing F1. Alternatively, read the window explanations in Table 4 on page 66.

If you want to start the driver now, select the **Yes** radio button. If you prefer to start it at a later time, select the **No** radio button. It is recommended that you configure all drivers before starting any of them.

4 Select one of the following **Keep Previous Configuration** radio buttons:

Yes Select this radio button if you are adding a driver to a control point or a managed host.

No Select this radio button if you are adding the driver for the control database, or if you are adding the initial driver for a managed host.

> If you select **No**, any previously created drivers are removed and replaced.

5 Select the **Do** push button. The configuration process starts.

The driver updates are now complete.

> If you selected the **No** option for starting the drivers, you can start them now (manually) by entering:
>
> **/etc/rc.dhudrv**
>
> This command starts all drivers which have been configured, not just the one you finished configuring.

Configuring Watchdogs

DataHub can manage multiple databases on the control point or on managed hosts. The following procedure can configure the control database watchdog, add additional watchdogs to the control point, or add watchdogs to a managed host.

If you adding additional watchdogs to an existing DataHub workstation, make sure that the DataHub watchdog processes are not running. For more information, see "Checking Common DataHub Processes" on page 78.

You might need to follow the steps in this section several times.

> If you want to modify the configuration of a watchdog such that it will communicate with a new or different watchdog server, use the following procedures except select **No** for the **Keep Previous Configuration** radio button.
>
> Use the **No** selection with caution, because it removes all configured watchdogs.

To configure DataHub watchdogs:

1 Perform the steps in Chapter 5, "Configuring DataHub Components: Alternative Options" on page 43.

2 If you are creating new watchdogs (migrating watchdogs requires only the steps in Chapter 5, "Configuring DataHub Components: Alternative Options" on page 43), select the **Configure Watchdogs** radio button. A new window opens.

3 Fill in the window fields as appropriate. If you need assistance, open the online help by selecting or tabbing to a field and pressing F1. Alternatively, read the window explanations in Table 5 on page 67.

If you want to start the watchdog now, select the **Yes** radio button. If you prefer to start it at a later time, select the **No** radio button. It is recommended that you configure all watchdogs before starting any of them.

4 Select one of the following **Keep Previous Configuration** radio buttons:

Yes Select this radio button if you are adding a watchdog to a control point or a managed host.

No Select this radio button if you are adding the watchdog for the control database, or if you are adding a watchdog to a managed host.

If you select **No**, any previously created watchdogs are removed and replaced.

5 Select the **Do** push button. The configuration process starts.

The watchdog updates are now complete.

If you selected the **No** option for starting the watchdogs, you can start them now (manually).

Before you start the processes manually, kill all watchdog processes that are currently running. Enter the commands:

ps -ef | grep watchdog
kill -9 *PID*

where *PID* is the process number returned from the **ps** command. Repeat the **kill** command for each process listed.

Also, local evaluation processes must be running on a managed host before you can start watchdog processes. For more information, see "Checking Common DataHub Processes" on page 78.

To manually start watchdog processes, enter:

/etc/rc.dhuwdg

Chapter 6. Installing DataHub Managed Host Files

This chapter contains the procedures for installing a DataHub managed host. The instructions tell you how to move DataHub files from the distribution media to system directories on workstations.

> If you are installing DataHub as a SystemView feature, read the Installation information panel for DataHub on the SystemView CD Showcase for different installation instructions.

Typically, you will manage one or more hosts using DataHub. The steps in this section must be repeated for each workstation that will be a DataHub managed host. These steps are not required for the control point workstation.

You have two options for installing managed host files:

- If the managed host is close and has a CD-ROM attached, use the first procedure ("Installing Managed Host Files Using the Managed Host CD-ROM Drive").
- If the managed host does not have a CD-ROM drive or is remote, use the second procedure ("Installing Managed Host Files Using the Control Point CD-ROM Drive" on page 55). This procedure uses the **ftp** command to transfer install images to the host.

Installing Managed Host Files Using the Managed Host CD-ROM Drive

To install managed host files using the managed host drive:

1 Log in to the managed host. It is not necessary to be root.

> If you are re-installing or migrating a DataHub release, stop all DataHub processes:
>
> **ps -ef | grep** dh
> **kill -9** *PID*
>
> where *PID* is the process number returned from the previous **ps** command. Repeat the **kill** command for each process listed.

Additionally, if you are migrating a DataHub release, you must install the new DataHub release files into your existing DataHub directory.

2 Enter **df** on the command line. Ensure that you have 32 MB of space available in the file system that will contain DataHub files (*datahub_path*).

3 Insert and mount the DataHub CD.

4 AIX only: Optional:

If you want to use smit and installp to install DataHub files on the AIX operating system, follow this step. If you would prefer to create the DataHub directories with system commands and then use the **tar** command to install DataHub files, skip to step 5.

a Enter **smit**.

b Go through the smit installation panel selections until you reach the Install Software Products at Latest Available Level window.

c Use the **List** option and select **1.2.0.0 dhumh** as the product to install.

The files are placed in the directory /usr/lpp/dhumh. The workstation now has all the files required to configure a managed host.

d Read the README.DHU file in the readme directory. It contains last-minute changes that can affect DataHub installation and configuration procedures.

e Proceed to one of the following topics:

- DB2v1 DB2v2 Ora Syb managed hosts: Chapter 7, "Configuring a DataHub Managed Host" on page 59
- Ing managed hosts: Chapter 3, "Building DataHub INGRES Components" on page 23

Do either step 4 or step 5. Do not do both steps.

5 Create a directory for DataHub. Throughout the rest of the procedure, this directory is referred to as *managed_host_path*. The following examples use the default user directory as the location for this directory.

AIX	**cd** /u **mkdir** *managed_host_dir*
HP	**cd** /usr **mkdir** *managed_host_dir*

Sun	**cd** /opt **mkdir** *managed_host_dir*

where *managed_host_dir* is a name you choose (for example, datahub)

6 Make *managed_host_path* the current directory:

cd *managed_host_dir*

7 Extract the appropriate installation archives to the current directory:

AIX	**tar -xvf** /dev/*media_device*/aixmh.tar
HP	**tar -xvf** /dev/rmt/*media_device*/hpmh.tar
Sun	**tar -xvf** /dev/rmt/*media_device*/sunmh.tar

8 Read the README.DHU file in the readme directory. It contains last-minute changes that can affect DataHub installation and configuration procedures.

9 Proceed to one of the following topics:

- DB2v1 DB2v2 Ora Syb managed hosts: Chapter 7, "Configuring a DataHub Managed Host" on page 59
- Ing managed hosts: Chapter 3, "Building DataHub INGRES Components" on page 23

Installing Managed Host Files Using the Control Point CD-ROM Drive

In this section, you copy files from the CD-ROM at the control point to a temporary control point directory. Later, you copy files from this temporary directory to each managed host in your environment. Each managed host type (AIX, HP-UX, Solaris) requires a specific set of files.

To copy files from the DataHub media using the control point drive:

1 Log in to the control point as root.

2 Enter **df** on the command line. Ensure that you have 16 to 48 MB of space in the file system that will contain DataHub files (*datahub_path*). You will need 16 MB of space for each managed host type (AIX, HP-UX, Solaris) you intend to use in your environment.

3 Create a temporary directory to extract the files before you transfer them:

mkdir *datahub_path*/tmp

4 Copy the necessary files from the archive on the control point. The system types shown in these examples indicate the system type of the managed host:

AIX	Change to the temporary directory: **cd** *datahub_path*/tmp Extract one of the following files: • If you intend to use **installp** commands at the managed host, copy the image file: **cp** *media_device*/dhumh.pkg . • If you will not use **installp** commands at the managed host, copy the tar archive: **cp** *media_device*/aixmh.tar .
HP	**cd** *datahub_path*/tmp **cp** *media_device*/hpmh.tar .
Sun	**cd** *datahub_path*/tmp **cp** *media_device*/sunmh.tar .

Throughout the rest of this procedure, this file is referred to as *archive_file*.

At this point you must now move the files from the control point workstation to the managed hosts.

To transfer the files:

1 Log in to the managed host as root.

If you are re-installing or migrating a DataHub release, stop all DataHub processes:

ps -ef | grep dh
kill -9 *PID*

where *PID* is the process number returned from the previous **ps** command. Repeat the **kill** command for each process listed.

Additionally, if you are migrating a DataHub release, you must install the new DataHub release files into your existing DataHub directory.

2 Enter **df** on the command line. Ensure that you have 16 MB of space available in the file system that will contain DataHub files (*datahub_path*).

3 Create a directory for DataHub. Throughout the rest of the procedure, this directory is referred to as *managed_host_path*. The following examples use the default user directory as the location for this directory.

AIX	**cd** /u **mkdir** *managed_host_dir*
HP	**cd** /usr **mkdir** *managed_host_dir*
Sun	**cd** /opt **mkdir** *managed_host_dir*

where *managed_host_dir* is a name you choose (for example, dhumh).

4 Make *managed_host_path* the current directory:

cd *datahub_dir*

5 Use the **ftp** command to log in to the control point workstation. It is not necessary to be root. A prompt similar to ftp> appears.

6 On the control point workstation, change to the temporary directory you created in step 3 on page 55.

ftp> **cd** *datahub_path*/tmp

7 Set the file transfer mode to binary:

ftp> **binary**

8 Copy the file to the managed host:

AIX (installp)	ftp> **get** dhumh.pkg
AIX (tar)	ftp> **get** aixmh.tar
HP	ftp> **get** hpmh.tar
Sun	ftp> **get** sunmh.tar

9 Quit the ftp session:

quit

10 AIX only: Optional:

If you want to use smit and installp on the AIX operating system to extract the file contents and discard the archive, follow this step. If you would prefer to use the **tar** command to extract DataHub files, skip to step 11 on page 58.

a Enter **smit**.

b Go through the smit installation panel selections until you reach the Install Software Products at Latest Available Level window.

c Use the **List** option and select **1.2.0.0 dhumh** as the product to install.

The files are placed in the directory /usr/lpp/dhumh. The workstation now has all the files required to configure a managed host.

d Remove the archive file:

rm *archive_file*

e Read the README.DHU file in the readme directory. It contains last-minute changes that can affect DataHub installation and configuration procedures.

f Proceed to one of the following topics:

- DB2v1 DB2v2 Ora Syb managed hosts: Chapter 7, "Configuring a DataHub Managed Host" on page 59
- Ing managed hosts: Chapter 3, "Building DataHub INGRES Components" on page 23

Do either step 10 on page 57 or step 11. Do not do both steps.

11 Use the **tar** command to extract the file contents and discard the archive:

tar -xvf *archive_file*
rm *archive_file*

12 Proceed to one of the following topics:

- DB2v1 DB2v2 Ora Syb managed hosts: Chapter 7, "Configuring a DataHub Managed Host" on page 59
- Ing managed hosts: Chapter 3, "Building DataHub INGRES Components" on page 23

Chapter 7. Configuring a DataHub Managed Host

You can configure one or more managed hosts for management by DataHub. The instructions in this chapter show you how to configure one managed host; therefore, you might have to go through these instructions several times if you are managing several hosts.

After configuration is finished, a DataHub control point can manage the host (you can add the managed host to the control point GUI). For more information, see the *DataHub for UNIX Operating Systems User's Guide*.

For all configuration activities on all workstations, you will use one of two programs: dhuinst or dhuinstty. The instructions in this chapter refer to dhuinst.

Preparing to Configure a Managed Host Component

This section lists information you need to collect and prerequisite steps for configuring a DataHub managed host.

1 Collect the following information:

- The managed database (on the host) name
- The managed database location:

DB2v1 and DB2v2	The instance name
Ing	The INGRES RDBMS installation directory name (the value of II_SYSTEM)
Ora	The directory name (the value of the ORACLE_HOME environment variable)
Syb	The directory name (the value of the SYBASE environment variable)

- Syb only:
  - The name of the Sybase server that holds one or more databases to manage.
  - The Sybase server login name and password that will be used to access Sybase. This Sybase login must have access to all managed databases, including the master database. The level of authority required is dependent on the watchdog checks.

Typically, the level is an SA role. The login is used by the Sybase database watchdog.

- The name of the host where the watchdog server is located
- The database watchdog user ID:

DB2v1 and DB2v2	A database user ID that has SYSADM authority.
Ing	A database user ID, defined using the accessdb utility, that has the authority to perform watchdog checks. This user should have DBA authority.
Ora	A database user ID that is externally identified. This ID must have authority (typically, DBA level) to perform watchdog checks.
Syb	This ID is the user ID that the watchdog process for Sybase runs under (the ID that started the process). This user ID can be an ordinary UNIX user ID.

2 Ensure that you have TCP/IP connectivity between the control point workstation and the managed host.

3 Check your umask setting. The umask setting can affect the installation of DataHub. For example, a umask of 027 causes some of the files built by the installation procedure to have the wrong permissions. Most DataHub files require permissions of 755; therefore, the maximum umask setting is 022. To see your current umask setting, type **umask**.

4 Optional: Add symbolic links to the local DataHub X resource definition file:

AIX	**cd** /usr/lib/X11/app-defaults **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn **ln -s** *datahub_path*/AIX/startup/XDhuInstall XDhuInstall **ln -s** *datahub_path*/AIX/startup/XStatus XStatus **ln -s** *datahub_path*/AIX/startup/XWarn XWarn

HP	**cd** /usr/lib/X11/app-defaults **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn **ln -s** *datahub_path*/HP-UX/startup/XDhuInstall XDhuInstall **ln -s** *datahub_path*/HP-UX/startup/XStatus XStatus **ln -s** *datahub_path*/HP-UX/startup/XWarn XWarn
Sun	**cd** /opt/SUNWmotif/lib/app-defaults **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn **ln -s** *datahub_path*/SunOS/startup/XDhuInstall XDhuInstall **ln -s** *datahub_path*/SunOS/startup/XStatus XStatus **ln -s** *datahub_path*/SunOS/startup/XWarn XWarn

5 Optional: Change the owner and group of the DataHub directories and executables from the default of root:sys. You can change these to another valid user ID and group on your system. The following example changes owner and group to bin:

chown -R bin:bin *datahub_path*

You are now ready to begin configuring the managed host components.

Configuring a Managed Host

To configure the components for a managed host:

1 Log in at the managed host as root.

2 Set the locale to a valid language (other than C or POSIX). For example:

export LANG=En_US

You can enter the **locale -a** command to determine which languages are installed on your workstation.

3 Set the NLS path.

The following statement (in Korn shell syntax) can be used to set the path:

export NLSPATH=$NLSPATH:*datahub_path/system_dir/*msg/%L/%N:\
*datahub_path/system_dir/*msg/C/%N

An example statement is:

export NLSPATH=$NLSPATH:/usr/lpp/dhu/AIX/msg/%L/%N:\
/usr/lpp/dhu/AIX/msg/C/%N

4 If you are configuring DataHub with LANG=Ja_JP or LANG=zh_CN and you started X Windows using some other setting, modify the DataHub configuration resource files (XDhuInstall, XStatus and XWarn):

a Enter: **cd** *datahub_dir/system_dir/*startup

b For Japanese, edit the resource files and add the following line:

```
*fontList : *-gothic-*:
```

c For Simplified Chinese, edit the resource files and add the following line:

```
*fontList : *-song-*:
```

d Set up your system to use these resource files. Do one of the following steps:

- Copy the resource files to root's home directory.
- Add a symbolic link from the app-defaults directory to the resource files. See step 4 on page 60.
- Set (and export) XAPPLRESDIR to the DataHub startup directory using the following command:

  export XAPPLRESDIR=*datahub_dir/system_dir/*startup

5 Start the configuration program:

a Change to the correct directory:

cd *datahub_path*/*system_dir*/install

b Enter one of the following commands:

- For hosts that support the X Window System and OSF/Motif:

  ./dhuinst

- For other hosts:

  ./dhuinstty

A window appears (Figure 14 on page 63).

Figure 14. DataHub Main Installation Window

At this point, you must decide if you are migrating your existing DataHub managed host to a newer release of DataHub or configuring a new managed host.

If a managed host configuration does not currently exist on this workstation, you must select the first option (**New Installation**). You can also use this option to replace an existing managed host configuration.

The migration procedure (**Upgrade Installation**) re-uses configuration data currently located in your system files. Migrating data will simplify your configuration process (the program finds values on your system instead of waiting for your input) and preserve many aspects of your current DataHub environment. Current watchdog and driver information is retained.

Migration is supported only from DataHub Release 1.1 to DataHub Release 2. For more information, refer to "Migration Considerations" on page 37.

Do one of the following steps:

a To configure a new managed host or replace an existing managed host configuration, select the **New Installation** radio button.

Continue with "Configuring a New DataHub Managed Host" on page 64.

b To migrate your current managed host, select the **Upgrade Installation** radio button. Next, select the **Upgrade Custom Installation** radio button. A new window opens (Figure 15 on page 64).

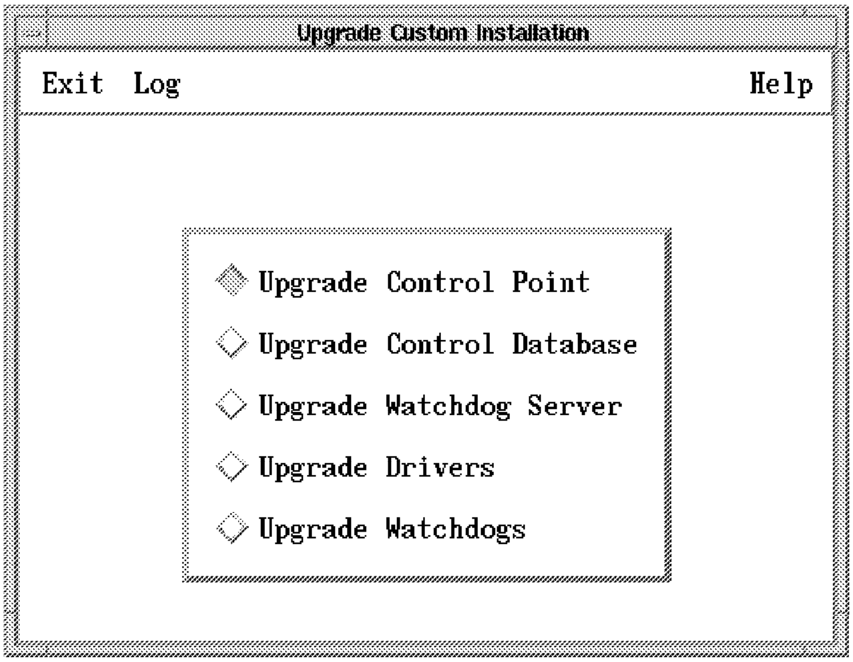

Figure 15. Upgrade Custom Installation Window

Select the **Upgrade Drivers** radio button.

Select the **Upgrade Watchdogs** radio button.

Your managed host is now upgraded. Continue with "Checking Managed Host Configuration or Migration Results" on page 69.

Configuring a New DataHub Managed Host

This section contains the configuration procedure steps you follow after starting the dhuinst program and selecting the **New Installation** radio button in the first window.

To configure a new DataHub managed host:

1 Select the **Configure Custom Installation** radio button. A new window opens (Figure 16 on page 65).

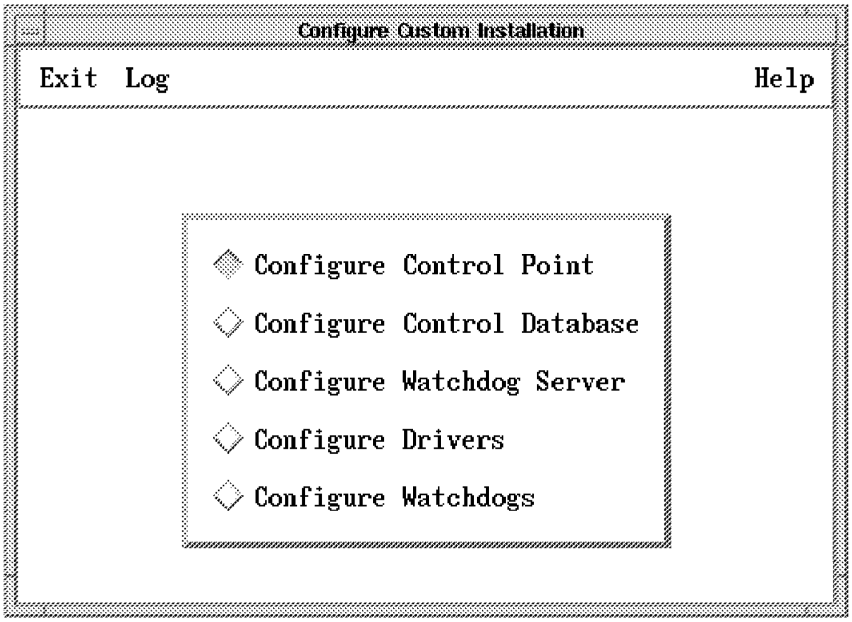

Figure 16. Configure Custom Installation Window

2 Select the **Configure Drivers** radio button. The window in Figure 17 opens.

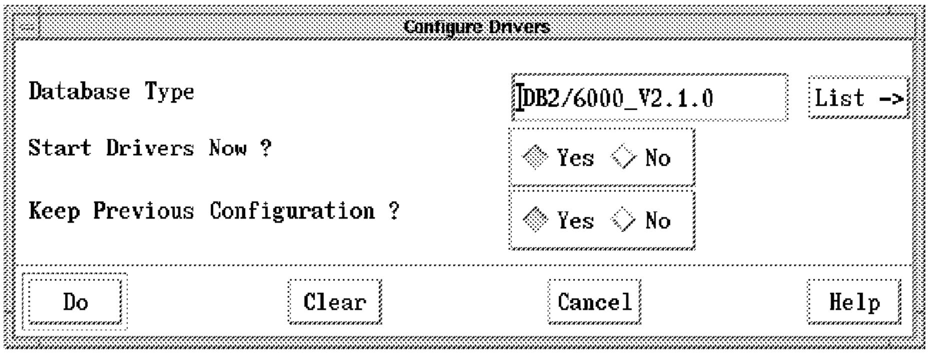

Figure 17. Configure Drivers Window

3 Fill in the field on the window. Table 4 on page 66 lists the information required for the one field.

If you need further assistance, refer to the online help.

Table 4. Field in the Configure Drivers Window	
Field	***Action***
Database Type	Select the **List ->** push button and then select the type of database to manage.

4 Select the **Yes** radio button for the **Start Drivers Now ?** field.

Selecting this option starts the script rc.dhudrv, which starts the operating system and database drivers

5 Select the **No** radio button for the **Keep Previous Configuration ?** field.

Selecting this option replaces any drivers previously configured for this workstation.

6 Select the **Do** push button. Your managed host driver configuration process starts.

> If DataHub was previously installed, several windows will appear asking if you want to continue or replace various soft links. Choose to replace the links.

When the program finishes, you should see Figure 16 on page 65.

7 Repeat steps 2 on page 65 through 6 for each additional RDBMS type.

8 Select the **Configure Watchdogs** radio button. The window in Figure 18 on page 67 opens.

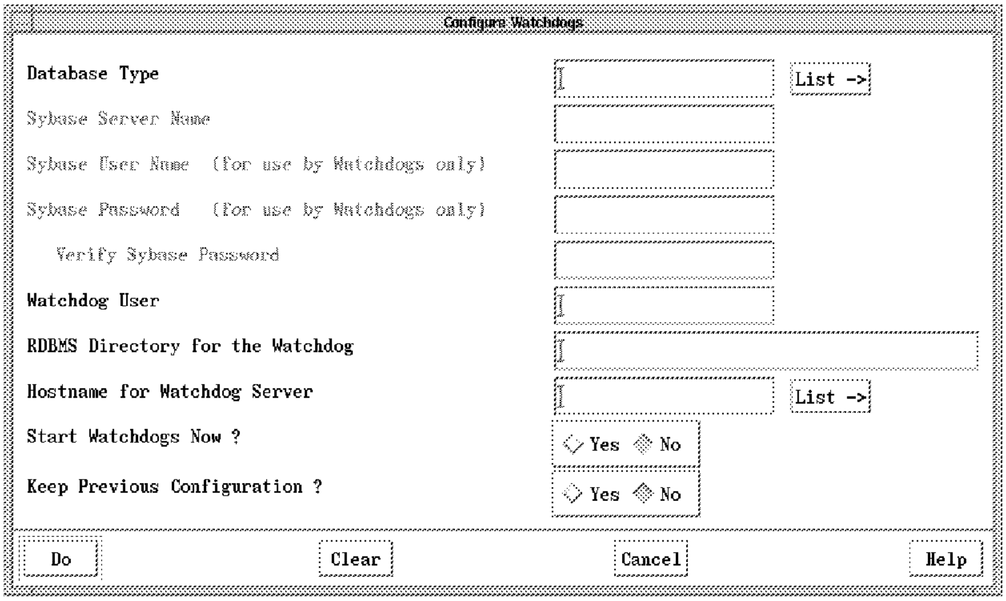

Figure 18. Configure Watchdogs Window

9 Fill in the fields on the window. Table 5 lists the information required for each field. Certain fields are database dependent and appear only when their associated RDBMS type is selected.

If you need further assistance, refer to the online help or, for general watchdog information, "Operating System and Database Watchdogs" on page 4.

Table 5 (Page 1 of 2). Fields in the Configure Watchdogs Window	
Field	***Action***
Database Type	Select the **List ->** push button and then select the type of database to manage.
Sybase Server Name (for use by Watchdogs only)	Syb Type the name of the Sybase Server.
Sybase User Name (for use by Watchdogs only)	Syb Type the Sybase server login name to use to access Sybase. This Sybase login should have access to all managed databases, including the master database. The level of authority required is dependent on the watchdog checks. Typically, the level is an SA role. The login is used by the Sybase database watchdog.

Table 5 (Page 2 of 2). Fields in the Configure Watchdogs Window	
Field	***Action***
Sybase Password (for use by Watchdogs only)	Syb Type the password for the Sybase server login name.
Verify Sybase Password	Syb Retype the login name password.
Watchdog User	Type the user ID to be used by the watchdog: DB2v1 Type a database user ID that has SYSADM authority. DB2v2 Type a database user ID that has SYSADM authority. In the instance owner's default environment, the variables user and db2instance must be set to the instance name. Ing Type a database user ID, defined using the accessdb utility, that has the authority to perform watchdog checks. This user should have DBA authority. Ora Type a database user ID that is externally identified. This ID must have authority to perform watchdog checks. Syb Type a user ID. This ID is the user ID that the watchdog process for Sybase runs under (the ID that started the process). This user ID can be an ordinary UNIX user ID.
RDBMS Directory for the Watchdog	Ing Type the directory corresponding to the II_SYSTEM environment variable for the INGRES RDBMS that this watchdog is responsible for. Ora Type the directory location of the databases that this watchdog is responsible for (the directory location should match the value of the ORACLE_HOME environment variable for this host). Syb Type the location of the Sybase server that contains the managed database for this watchdog (the location should match the value of the SYBASE environment variable for this host).
Database Instance Name for the Watchdog	DB2 Type the name of the database instance that owns one or more managed databases that are to be monitored.
Hostname for Watchdog Server	Type the name of the host where the watchdog server is located.

10 Select the **Yes** radio button for the **Start Watchdogs Now ?** field.

Selecting this option starts the operating system and database watchdogs.

11 Select the **No** radio button for the **Keep Previous Configuration ?** field.

Selecting this option replaces any watchdogs previously configured for this workstation.

12 Select the **Do** push button. Your managed host configuration process starts.

> If DataHub was previously installed, several windows will appear asking if you want to continue or replace various soft links. Choose to replace the links.

Checking Managed Host Configuration or Migration Results

To check your results:

1 Check the install log to make sure the operation was successful. You can do this from within the configuration program by selecting **View** from the **Log** menu of the Configuration Menu (new configuration) window or the Upgrade Menu (migration) window.

You can check the install log at any time. One method of viewing the file is:

cat *datahub_path*/*system_dir*/install/install.log **| pg**

You might want to copy this log file, because it is over-written each time the configuration program is started.

> The install log contains the password used for the Sybase server; therefore, use discretion if you reference this file. Two other files generated by the installation program, general.mem and local.mem, also contain password information and should be protected. For more information, see Appendix C, "DataHub Passwords" on page 100.

2 Optional: If you require more watchdogs (you will need additional watchdogs if you want to manage two or more databases on the control point), see the instructions in "Configuring Watchdogs" on page 51.

3 Quit the root command shell:

exit

The workstation is configured and ready for management by your control point. You must, however, add this managed host to the control point GUI before you can manage it. Add this host by selecting the **Host** object type and then selecting the **Add** button.

If your control point GUI cannot recognize this managed host, it is probably because one or more processes were not started. For more information, see Chapter 9, “Troubleshooting DataHub Conditions and Messages” on page 78.

Chapter 8. Customizing Your DataHub Environment

This chapter contains procedures that you can perform after you install DataHub:

If You Want To	***See***
Customize DataHub	"Changing DataHub Settings"
Start DataHub from Netview	"Enabling a Netview Launch of DataHub on AIX and Solaris" on page 73
View DataHub softcopy books	"Installing IPF/X Softcopy Book Support for DataHub" on page 74

Changing DataHub Settings

You can customize many of DataHub's attributes. This section explains how to set:

- DataHub PostScript printers
- DataHub X Resources
- DataHub operating system watchdog users

Defining a PostScript Printer

You can define a PostScript printer for output from DataHub either during configuration (using dhuinst or dhuinstty) or after configuration (by following these instructions).

Use a text editor to enter a line with the necessary printer information into the *datahub_path*/*system_dir*/gui/apps.pl file. The syntax of the line is:

printer(*hostname*, *queuenumber*, *queuename*, *outputtype 'description'*).

Where:

hostname
: Represents the name of a DataHub managed host (which might or might not be the control point), where the printer queue is defined to the operating system.

queuenumber
: Represents the queue number, as a positive integer, for this printer at this host. You can define many printers on each host. Each printer will have a unique queue number defined for DataHub. This number is for

DataHub use only and is not required to correspond with a definition of the printer to the operating system.

queuename
Represents the name of the printer queue as defined in the /etc/qconfig file on *hostname*. This name is displayed as a choice when you select a printer (from the control point GUI) for your output.

outputtype
Represents the type of output. Only ps (PostScript) is supported.

description
Represents a short description that will appear in the DataHub print window.

> The parentheses and period at the end of the printer information line are required elements.

Changing X Resources

You can change many of DataHub's interface attributes by editing the X resource file, XDataHub. These attributes include font type, colors, window size, window position, and others. For example, to change the background color of the DataHub windows:

1. Open the file *datahub_path*/*system_dir*/startup/XDataHub in a text editor.
2. Find the line containing the background attribute: *background
3. Change the value to the right of the colon to the color you want displayed.

Now, each time a DataHub window is displayed, the new background color will appear. For more information on altering X Resources, refer to *DataHub for UNIX Operating Systems User's Guide* and the X System and OSF/Motif manuals specific to your operating system.

Changing the User for the Operating System Watchdog

The operating system watchdog and database watchdog are both run with the user ID supplied for the watchdog user. This user ID is a database or instance owner ID. If you want the operating system watchdog to run with a different user ID, you need to change the file /etc/rc.dhuwdg, stop the watchdog processes, and restart the watchdogs.

After switching to root, change the next to the last line from:

start_watchdog os *old ID* dummy dummy

to:

start_watchdog os *new ID* dummy dummy

where *new ID* is the ID you want.

Refer to "Checking Common DataHub Processes" on page 78 for more information on understanding and starting watchdog processes.

Enabling a Netview Launch of DataHub on AIX and Solaris

On AIX and Sun Solaris systems, DataHub can be launched from NetView.

To enable a NetView launch for DataHub, you must follow one of two different procedures.

- AIX Configure a control point on an AIX system. Configuring a control point on AIX automatically enables DataHub for a NetView launch. See "Configuring a Control Point" on page 29.
- Sun Follow these procedures:
  1. From the control point, log in as root.
  2. Edit datahub.lf to set the INSTALL environment variable to *datahub_path*/*system_dir*.
  3. If your system uses a directory path for NetView other than /usr, edit *datahub_path*/nvlaunch/datahub.arf to replace each instance of /usr with your NetView home directory path. This value is your *netview_path*. NetView installation instructions recommend the value /usr, but your system might use a custom directory path.
  4. Create soft links to DataHub's NetView files in the appropriate NetView directories.

     cd *netview_path*/OV/registration/C
     ln -s *datahub_path*/nvlaunch/datahub.arf datahub.arf

     cd *netview_path*/OV/bin
     ln -s *datahub_path*/nvlaunch/datahub.lf datahub.lf

     cd *netview_path*/OV/icons/gifs
     ln -s *datahub_path*/nvlaunch/dhlogo.gif dhlogo.gif

     cd *netview_path*/OV/icons/drag-bitmaps
     ln -s *datahub_path*/nvlaunch/dhubnew.xbm dhubnew.xbm

Start NetView. The DataHub icon appears in the Tools window and a **DataHub** menu choice appears in the **Tools** menu of the Submap window.

To launch DataHub from the NetView Tools window, drag the **DataHub** icon (with the middle mouse button) to the desktop.

To launch DataHub from the Submap window, select the **DataHub** menu choice from the **Tools** menu.

In either case, you will see Figure 11 on page 42.

Installing IPF/X Softcopy Book Support for DataHub

The IPF/X run-time package contains a program named xview that you can use to view DataHub books online.

This section explains how to install the package. Follow the instructions in the section that applies to your operating system:

- "Installing the IPF/X Run-Time Package on AIX"
- "Installing the IPF/X Run-Time Package on HP-UX" on page 75
- "Installing the IPF/X Run-Time Package on Sun Solaris" on page 77

Installing the IPF/X Run-Time Package on AIX

To install the IPF/X run-time package on AIX:

1 Login as root.

2 Insert the CD into a CD drive and mount it to the file system.

3 Use smit or installp to complete the installation:

- Using smit:

  a Start smit:

  smit install

  b Select installation options (in the following order):

  Install / Update Software
  Install / Update Selectable Software (Custom Install)
  Install Software at Latest Available Level

  c From the Input Device/Directory window, enter the device name or directory for the DataHub CD-ROM. For example:

  /dev/cd0

d Use the **List** option to select the IPF/X run-time packages for your system. One or more of the following values appear in the **SOFTWARE to Install** field:

1.1.0.0 ipfx (for the IPF/X run-time package and all NLS messages)

1.1.0.0 ipfx.Run-Time (for the IPF/X run-time package)

1.1.0.0 ipfx.nls.Ja_JP (for messages in Japanese)

1.1.0.0 ipfx.nls.zh_CN (for messages in simplified Chinese)

e Set the remaining entry fields to values appropriate to your installation. Some guidelines are:

- To be able to remove the IPF/X run-time package at a later time, select **no** for the **COMMIT software** field; otherwise, select **yes** for a permanent installation.
- Select **yes** for the **EXTEND file system if space is needed?** field.
- If you have a previously installed version of the IPF/X run-time package, select **yes** for the **OVERWRITE existing version?** field.

f Select **Enter** to install the IPF/X run-time package.

- Using installp:

  If you have a previous version of the IPF/X run-time package, use the following command:

  installp -aF -c -C -N -d /cdrom *ipfx_package*

  Otherwise, enter the following command:

  installp -ag -c -d /cdrom *ipfx_package*

  where *ipfx_package* is:

  ipfx.Run-Time (for IPF/X run-time package)
  ipfx.nls.Ja_JP (for messages in Japanese)
  ipfx.nls.zh_CN (for messages in simplified Chinese)

The IPF/X package is now installed.

Installing the IPF/X Run-Time Package on HP-UX

You can use the **update** command to install the IPF/X run-time package. The files are:

ipfhrun.pkg (the run-time files)
ipfhmsg.pkg (the run-time messages)

To install the IPF/X run-time package on HP-UX:

1. Login as root.
2. Insert the CD into a CD drive and mount it to the file system.
3. If you previously installed the IPF/X run-time package using the **update** command, follow these steps:
   a. Remove the files by executing the following commands:

      rmfn -l IPFR-RUN
      rmfn -l IPFR-MSG

   b. Proceed to step 5.
4. If an older version of the IPF/X run-time package is installed on your system, remove its files:
   a Find and remove the IPF/X home directory, ipfx or ipfxsdk. One way to find this directory is to list the directory information for one of the IPF/X executable file links. For example, if entering:

   ls -al /usr/bin/ipfc

   returns:

   lrwxrwxrwx 1 root system /usr/bin/ipfc@ -> /usr/lpp/ipfxsdk/bin/ipfc*

   then, remove the IPF/X home directory by entering:

   rm -r /usr/lpp/ipfxsdk

   b Remove the IPF/X links and supporting files:

   rm /usr/bin/xview
   rm /usr/bin/ipfc
   rm /usr/bin/ipfxref
   rm /usr/bin/ipfxug
   rm /usr/lib/libipfx.a
   rm /usr/include/ipfx.h

   rm /usr/include/hmtailor.rc or /usr/include/hmtailor.h
5. Use the **update** command to install the IPF/X run-time package:

   update -s /cdrom/ipfhrun.pkg IPFRRUN.IPFR-RUN
   update -s /cdrom/ipfhrun.pkg IPFRMSG.IPFR-MSG

The IPF/X package is now installed.

Installing the IPF/X Run-Time Package on Sun Solaris

You can use the **pkgadd** command to install the IPF/X run-time package. The file to install is ipfspkg.tar.

To install the IPF/X run-time package on Sun:

1 If an older version of the IPF/X run-time package is installed on your system, remove its files:

a. Find and remove the IPF/X home directory, ipfx or ipfxsdk. One way to find this directory is to list the directory information for one of the IPF/X executable file links. For example, if entering:

ls -al /usr/bin/ipfc

returns:

lrwxrwxrwx 1 root system /usr/bin/ipfc@ -> /opt/ipfx/bin/ipfc*

then, remove the IPF/X home directory by entering:

rm -r /opt/ipfx

b. Remove the IPF/X links and supporting files:

rm /usr/bin/xview
rm /usr/bin/ipfc
rm /usr/bin/ipfxref
rm /usr/bin/ipfxug
rm /usr/lib/libipfx.a
rm /usr/include/ipfx.h
rm /usr/include/hmtailor.rc

2 Issue the following commands to install the IPF/X run-time package:

cd /tmp
tar -xvf /cdrom/ipfspkg.tar
pkgadd -d /tmp/pkg1

The **pkgadd** command prompts you to install either IPFR-RUN or IPFS-SDK. Select IPFR-RUN.

3 Remove the temporary files:

rm /tmp/ipfspkg.tar
rm -rf /tmp/pkg

4 Quit the root session:

exit

The IPF/X package is now installed.

Chapter 9. Troubleshooting DataHub Conditions and Messages

This chapter will help you solve problems that can appear when using DataHub. It has two sections:

- "Checking Common DataHub Processes" covers the most common error condition: key processes were not started.
- "Solving Configuration, Startup, and Usage Problems" on page 80 covers other common error conditions. It is organized by stages:
  - Configuration problems are first
  - Startup problems come next
  - Usage errors and other common error conditions are at the end

> The DataHub monitoring system logs error information to the system error log. If you are experiencing trouble with the watchdogs you should check to see if DataHub has logged any information to the system error log. All information logged by the monitoring system will be logged as warnings.

Checking Common DataHub Processes

DataHub requires several processes running on the control point before it can start. A subset of these processes is required on all managed hosts.

The most common cause of DataHub problems is that one or more of these processes were not started. It is possible, for example, that you chose not to start the database driver, watchdog, and possibly other processes when you configured DataHub.

Enter **ps -ef | grep** dh from either the control point or managed host command line. Write down the listed processes and compare them carefully to the processes listed in Table 6 on page 79.

Table 6. DataHub Processes (Superset)		
Name and Location	***Processes***	***Scripts***
Watchdog server. A major component of the control point that typically resides on the same workstation as the control point application. If you are checking processes from a managed host or a control point workstation that does not have this component (see "Configuring a Watchdog Server" on page 49), you will not see all of these processes; however, a subset of these processes will appear on managed hosts (see the list for local evaluation processes).	dhGComm dhLComm dhEval dhAction dhCDBAccess dhInfobase	rc.dhu_gcs rc.dhu_sms rc.dhu_ia
Operating system watchdog. One resides on each managed host (including the control point workstation).	watchdog.os	rc.dhuwdg
Operating system driver. One resides on each managed host (including the control point workstation).	osd	rc.dhudrv
Database watchdogs. One for each managed database instance. It resides on the workstation where the database is located, whether on the control point or on a managed host.	watchdog.db2v1 watchdog.db2v2 watchdog.ora7 watchdog.syb watchdog.ing64	rc.dhuwdg
Local evaluation processes. One set of these processes resides on each managed host. They provide support for the watchdogs at the managed host.	dhLComm dhEval dhAction	rc.dhu_sms
Database driver. One for each RDBMS type on each managed host. It resides on the workstation where the RDBMS is located, whether on the control point or on a managed host.	db2v1d db2v2d (HP and Sun) db2v210d (AIX only) db2v211d (AIX only) ora7d sybd ing64d	rc.dhudrv

Evaluate your situation. You don't have to have all of the listed processes running on your workstation for DataHub to work. For example, you don't need to have database driver processes running for databases that do not exist on a managed system. And if you decided to use an alternative setup, such as placing your watchdog server on one workstation and your control point on another, your process list will vary.

If you determine that one or more processes is missing, and the table indicates that your configuration should have them, start one or more now by entering one of the following command sets (you must be root to enter these commands):

- Control point root users must enter (in the following order):

  /etc/rc.dhudrv
  /etc/rc.dhu_gcs
  /etc/rc.dhu_sms
  /etc/rc.dhu_ia
  /etc/rc.dhuwdg

- Managed host root users must enter (in the following order):

  /etc/rc.dhudrv
  /etc/rc.dhu_sms
  /etc/rc.dhuwdg

Verify that all required processes are now running.

Solving Configuration, Startup, and Usage Problems

Search the headings for symptoms that match your current error condition. Then, evaluate possible causes listed on the left side and attempt solutions listed to the right of each possible cause.

Symptom: DataHub configuration fails.

Possible Cause	Recommended Action
Undefined host type.	If you receive a message stating that you have an undefined host type, a possible cause is that the **uname -s** command is returning too much data. To bypass the command, edit the file *datahub_path*/*system_dir*/install/config_cp and change the line containing OSTYPE=‘uname -s’ to one of the following lines as appropriate: • OSTYPE=‘AIX’ • OSTYPE=‘HP-UX’ • OSTYPE=‘SunOS’

Symptom: DataHub does not migrate an existing configuration.	
Possible Cause	**Recommended Action**
Transaction failure.	Check the log file (install.log). Migration transaction failures are written to the log file and should provide information about the cause. The migration program SQL statements use a “insert into... as select from...” structure. The migration procedure processes the migration of all rows in a single table into a single transaction. If one row fails, the entire transaction fails. A typical cause is that the space allocated for logging is not large enough to handle the transaction. Refer to your RDBMS documentation for information on increasing the available space for logging.

Symptom: DataHub does not start.	
Possible Cause	**Recommended Action**

The file, datahub, cannot be found.	See if the program runs from the *datahub_dir*:
	
	cd *datahub_dir*/*system_dir*/gui
	./datahub
	
	If it starts, then datahub, or its link, might not be in the path of the system. If a link for datahub was not created during configuration, check that *datahub_path* is in the path:
	
	echo $PATH
	
	If a link was created:
	
	• Check that the link was created and that it is pointing to the correct directory (*datahub_path*/*system_dir*/gui):
	  ls -l /usr/bin/datahub
	• Ensure that /usr/bin is in the path.
	  echo $PATH

Symptom: DataHub does not start.	
Cannot open display.	If you receive a message stating that the display cannot be opened, reset the environment display variable. Check the current display setting: **echo** $DISPLAY Set the display (Korn shell syntax): export DISPLAY=*hostname*:*N* where *hostname* is the name of the X-Station or host where *you* are physically located (the TCP/IP-connected workstation where you want to display DataHub). If the host is in a different domain, supply either the full DNS name or IP address. *N* is the screen number (0 if only one screen is connected to this station). Refer to the X Window System manuals for more information.
The Motif window manager is not active.	Ensure that the Motif window manager process (mwm) is running on your workstation (or the workstation handling the X interface, that is, the X server): **ps -ef | grep** mwm If mwm is not active, start it by entering one of the following commands: • **startx** • **xinit**
Bad connection.	A connection can be refused when you try to start DataHub from a remote workstation. Enter the following command in a shell running from the X server workstation (the workstation where you initiated the **startx** or **xinit** command): **xhost +** This command allows any remote X client application, such as DataHub, access to your workstation. Alternatively, you can limit access to only those X client applications running from a named workstation with the command: **xhost +***workstation_name* where *workstation_name* is the name of the control point workstation. If the control point is in a different domain than the X server workstation, you must add the workstation name to the X server host file.
The client is not authorized to connect to the server.	Include the local workstation name in the xhost file.

Symptom: DataHub does not start.	
Drivers not started.	There are several drivers used by DataHub. These drivers must be active before starting the control point application. It is possible that one or more drivers did not start when the system was booted. Verify that the minimum processes are active, and start those that aren't. See Table 6 on page 79 for a list of the processes that should be running on a control point with all the components. If you configured DataHub using a custom configuration, be sure to check the process list on each of the workstations containing a control point component. If you need to start processes (refer to "Checking Common DataHub Processes" on page 78 for more information), start them in the order presented. To start the drivers now, run the following script file: **/etc/rc.dhudrv**

Symptom: DataHub does not start—receive 'killed' message, or system hangs.	
Possible Cause	**Recommended Action**
Paging or memory problems could occur when the background processes are started or when DataHub is started.	Check the paging space defined to the control point workstation. The recommended paging space is 2.5 to 3 times the amount of memory on the workstation.

Symptom: DataHub starts but fails immediately.	
Possible Cause	**Recommended Action**
Current user ID might not belong to one of the groups known to DataHub.	From an authorized user's session, check the current user's group authorization by selecting **User Management** from the **Privilege** menu. Refer to *DataHub for UNIX Operating Systems User's Guide* for more information.
Current workstation not defined in the host table of the workstation running the X server.	Check the host table of the serving workstation. The table should list the host name and TCP/IP address of the X client workstation.

Symptom: DataHub starts but fails immediately.	
If failure occurs after an SQL failure message appears, the user ID provided for login to the control database does not have authorization to the DataHub tables and views.	Ensure that the current user has permission to read information located in the control database. See *DataHub for UNIX Operating Systems User's Guide* for the procedure for authorizing users to access the control database.
LANG environment variable is not set to a language installed on your system.	DataHub uses the LANG environment variable to determine the language and code page to use. A valid LANG value must be set before DataHub starts. You might see one or more of the following messages on the window where you attempted to start DataHub: • nlsGetText cannot open cat • cannot open messages file • specify a valid language for your system • LANG=lang; export LANG (Bourne shell) • setenv LANG lang (C shell) To determine the languages that are available on your system, enter the following command: **locale -a**
AIX Installation of DataHub with installp failed to create the msg directory.	Using smit, re-install DataHub. Select "dhu ALL" as the software to install and ensure **Include corresponding LANGUAGE file sets?** is set to "Yes".

Symptom: Action buttons do not appear on the DataHub main window.	
Possible Cause	**Recommended Action**
The user ID used to access the control database is not defined to a group known to DataHub.	1. Select **DB Connections** from the **File** menu. 2. Select the entry for your host and control database. 3. Select the **Close** push button, then select the **Open** push button. 4. Select the host and control database from the list and be sure to use a user ID that belongs to a DataHub group.

Symptom: When a host or database object is selected, an error message appears.	
Possible Cause	**Recommended Action**

Symptom: When a host or database object is selected, an error message appears.	
The control point and managed host are using different port addresses.	This problem could be due to the entries made during installation, or during a TCP/IP refresh of the inetd process. To correct the problem: 1. Edit the /etc/services file on the control point and each managed host to ensure the socket port addresses match. Also, ensure a single entry is present for each of the DataHub services. 2. Force a refresh of the inetd process on the control point and each managed host: **refresh -s** inetd

Symptom: Error occurs during login to DataHub.	
Possible Cause	**Recommended Action**
If you receive the error message: "Connect failed with error '-1'," the user login is incorrect.	Ensure you are using a correct login for the control database owner.
If you receive the error message: "Cannot connect to database driver," with an error level of -2, the database driver for the control database is not active.	Start the database driver by entering the following command from the workstation where the control database resides: **/etc/rc.dhudrv**
If you receive the error message: "Connect failed with error -3, 'attempting to use newer protocol'," the control point application is at a later level than the database driver for the control database.	On the workstation where the control database is located, configure the database driver that is at the same release level as the control point application.

Symptom: DataHub fails, terminates execution.	
Possible Cause	**Recommended Action**
The shell from which you started DataHub was killed.	Restart DataHub; do not kill the DataHub startup shell.

Symptom: Error occurs when you attempt a database action.	
Possible Cause	**Recommended Action**
If you receive the error message: "Connect failed with error -2," the database driver for the RDBMS type of the selected database is inactive.	Start the database driver by entering the following command from the workstation where the managed database resides: **/etc/rc.dhudrv**
If you receive the error message: "Connect failed with error -3, 'attempting to use newer protocol'," the control point application is at a later level than the database driver.	On the workstation where the managed database is located, configure the database driver that is at the same release level as the control point application.
If you receive the error message: "Connection refused, error code -1," the rexec command might be disabled at the managed host.	On the workstation where the managed database is located, enable the rexec command.

Symptom: Error occurs when you attempt an operating system action.	
Possible Cause	**Recommended Action**
If you receive the error message: "Remote command for host '*hostname*' failed with error message 'workstation unreachable'," the operating system driver for the control point is not active.	Start the operating system driver by entering the following command on the workstation you are attempting to access, whether it be the control point or a managed host. **/etc/rc.dhudrv**
Host is unknown to DataHub.	Check the network server to see if a host was incorrectly specified. Verify (using the **ping** command) TCP/IP communication between the managed host and the control point. Issue the **ping** command from both the managed host and the control point using the host names displayed in the DataHub window. The command syntax is: **ping** *hostname*

Symptom: DataHub hangs, and communications problems arise.	
Possible Cause	**Recommended Action**
One or more DataHub drivers are not active.	Check the active processes by issuing the following command on the workstation where the control point application resides: **ps -ef | grep** dh Verify the minimum processes are active, and start those that aren't. See Table 6 on page 79 for a list of the processes that should be running on a control point with all the components. If you installed DataHub using a custom installation, be sure to check the process list on each of the workstations containing a control point component.
TCP/IP connection problem.	Verify (using the **ping** command) TCP/IP communication between managed hosts and the control point. Issue the **ping** command either from all managed hosts to the control point or from the control point to all managed hosts. The command syntax is: **ping** *hostname* If packets are not received, ask your network administrator to find the break in the link. If there is no break in the network, check the port addresses in the file /etc/services, and ensure the control point and managed hosts are using the same socket port addresses for each DataHub service. Also, verify that each DataHub process has a unique port address and that each service is assigned a unique port address. AIX You can force a refresh of the ports by issuing the following command on the control point and managed host workstations: **refresh -s** inetd

Symptom: Unable to start one or more DataHub components.	
Possible Cause	**Recommended Action**
TCP/IP port is in use.	The DataHub drivers will not start if the port assigned them is already in use. Check the status of the ports by entering the following command: **netstat -a | grep** *service* where *service* is one of the DataHub services by name (for example, osd).

Symptom: Incomplete icons in the DataHub Main Window.	
Possible Cause	**Recommended Action**
The current icon font is too large.	Select a smaller font size by updating the XDataHub file located in *datahub_path*/*system_dir*/startup

Symptom: Watchdog server fails to start.	
Possible Cause	**Recommended Action**
The control database RDBMS is not active.	The watchdog server will not start unless the RDBMS containing the control database is already active and the DataHub database driver for that RDBMS type is active. Refer to your RDBMS documentation for procedures on starting the RDBMS. See "Checking Common DataHub Processes" on page 78 for information about DataHub processes.
Watchdog server is not running.	There should be an entry in the /etc/inittab file that starts the watchdog server on workstation reboot; check the file to ensure the entry is there (unless you decided previously to remove an entry). Then, check to see if the watchdog server processes are currently running by entering the following command on the workstation where the watchdog server resides: **ps -ef | grep** dh Compare the results with Table 6 on page 79. If the processes are not running, start them by entering the following commands from the workstation where the watchdog server resides: **/etc/rc.dhu_gcs** **/etc/rc.dhu_sms** **/etc/rc.dhu_ia**
User specified as the database owner cannot access the control database tables.	The database owner and password specified during the configuration process are used for the watchdog server's access to the control database. Check the /etc/rc.dhu_ia file to determine the user ID (search for the CDBOWNER variable) used by the watchdog server. Check the *datahub_path*/*system_dir*/server/CDBAccess file to determine the password used by the watchdog server. If the password of the control database owner changed, update the CDBAccess file with the new password for the watchdog server. For more information, see "Watchdog Server Password" on page 100.

Symptom: Watchdog server fails to start.	
The database driver for the control database is not active.	1. Verify the database driver is active: **ps -ef | grep** dh See Table 6 on page 79 for the processes to look for. 2. If the driver is not running, start it by entering the following command from the workstation where the control database resides: **/etc/rc.dhudrv** 3. Start the watchdog server by entering the following commands from the workstation where the watchdog server resides: **/etc/rc.dhu_gcs** **/etc/rc.dhu_sms** **/etc/rc.dhu_ia**

Symptom: No values are returned for an operating system or database check.	
Possible Cause	**Recommended Action**
Check value storage was not enabled.	Define a check with the **Store check values** radio button set to **Yes**.
Watchdog server is not running.	On the workstation where the watchdog server resides, check to see if its processes are running: **ps -ef | grep** dh Compare the results with Table 6 on page 79. If the watchdog server is not running, start it by entering the following commands from the workstation where the watchdog server resides: **/etc/rc.dhu_gcs** **/etc/rc.dhu_sms** **/etc/rc.dhu_ia**
Filter is being used, and check values never pass through the filter.	Verify that the watchdog check should be returning values. Check the start time, end time, interval, and filter for the check. Test the check and see what value is returned; if the check filter is not met, the check value will not be sent to the watchdog server.

Symptom: No values are returned for an operating system or database check.	
Watchdog processes and local evaluation processes are not running on the system that the checks are defined for.	Verify that local evaluation processes and watchdog processes are active on the workstation where the checks are being performed: **ps -ef | grep** dhLComm **ps -ef | grep** dhEval **ps -ef | grep** dhAction **ps -ef | grep** watch If nothing is returned, start the local evaluation processes and watchdogs by entering the following commands: **/etc/rc.dhu_sms** **/etc/rc.dhuwdg**
Control point application is referencing a different control database than the watchdog server and watchdogs.	1. Check the /etc/rc.dhu_ia file on the watchdog server workstation. Find the name of the control database used by this watchdog server. 2. Ensure that this control database is the same one used by the control point application.
Watchdog user cannot run a check.	1. Enter the following command on the managed host where the watchdog resides: **ps -ef | grep** watch 2. Examine the output. The user, or Sybase login, listed in the output must have sufficient authority for running the check. For a Sybase watchdog, the -u flag in the output specifies the user ID that the Sybase watchdog uses to access a Sybase server. For all other watchdog types, column one of the output identifies the user that started the watchdog. The user, or Sybase login, must have sufficient authorization to run the check. For Oracle watchdogs, this user ID must be an Oracle externally identified user. 3. Log in with this user ID and run the check manually. 4. Verify that the check (operating system command, shell script, or SQL command) returns results of the expected type (integer, float, or string).

Symptom: DB2 watchdog check returns a -1.	
Possible Cause	**Recommended Action**

Symptom: DB2 watchdog check returns a -1.	
Required DB2 monitor switch is not active.	Standard monitoring for DB2 databases requires DB2 monitor switches to be active for valid information to be collected. If the standard monitoring is activated and DB2 monitor switches are not active, some of the standard checks will not collect valid data. The DB2 monitor switches which are required for standard monitoring are the Buffer Pool and Sort Monitor switches. These switches are activated/deactivated at the DB2 instance. Most pre-defined checks for DB2 use the DB2 snapshot monitor to collect information. Refer to the *DB2 for AIX Database System Monitor Guide and Reference* for details on the monitor switches and information which will be collected when each switch is active.
There are no connections to the database.	The DB2 snapshot monitor requires at least one active connection for the database. Establish a connection to the database and determine whether the check returns values.

Chapter 10. Removing DataHub from a Workstation

This chapter tells you how to remove DataHub from workstations.

The following procedure removes a DataHub control point. If you customized your DataHub control point, the procedure does not directly apply, because the components might reside on separate workstations. You can, however, use the following procedure as a guide for removing remote components.

To remove DataHub components from a managed host, bypass steps: 6, 9, 10, 12, 14, 15, and 16.

To remove a DataHub control point:

1 Log in as root.

2 Kill all DataHub processes:

ps -ef | grep *datahub_dir*

where *datahub_dir* is the truncated name of the directory where the DataHub files are located (the last directory name in *datahub_path*).

kill -9 *PID*

where *PID* is the process number returned from the previous **ps** command. Repeat the **kill** command for each process listed.

3 Remove the DataHub script files:

cd /etc
rm rc.dhudrv*
rm rc.dhu_gcs*
rm rc.dhu_sms*
rm rc.dhu_ia*
rm rc.dhuwdg*
rm dhu_cmd*
rm dhu_klog*

4 Edit the /etc/services file and remove all lines that contain DataHub port addresses.

> Make a backup copy of the file before editing it; for example:
>
> **cp** /etc/services /etc/services.bak

5 Edit the /etc/syslog.conf file and remove the entry local3.info.

6 Unlink the IPF/X library:

> Do this step if the soft link is pointing to the DataHub directory. Skip this step If the link is pointing to some other IPFX directory.

cd /usr/lib
unlink libipfx.a

7 Unlink the shared libraries:

AIX	**cd** /usr/lib **unlink** libdhu.o
HP	**cd** /usr/lib **unlink** libdhu.sl
Sun	**cd** /usr/lib **unlink** libdhu.so

8 Unlink the trap file:

cd /usr/bin
unlink dhtrap

9 Unlink the resource files:

> This step requires that you locate the X11/app-defaults directory. If you do not know the location of this directory, you might want to start a find process in another window while you manually search at the same time; for example:
>
> **xterm -e** ′**find** / **-name** app-defaults
> **-type** d **-print** > /tmp/find_results′ **&**

AIX	**cd** *app-defaults_dir* **unlink** XDataHub **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn where *app-defaults_dir* is probably one of the following files: • /usr/lib/X11/app-defaults • /usr/lpp/X11/lib/X11/app-defaults

HP	**cd** *app-defaults_dir* **unlink** XDataHub **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn where *app-defaults_dir* is probably one of the following files: • /usr/lib/X11/app-defaults • /usr/lib/X11R5/lib/X11/app-defaults
Sun	**cd** *app-defaults_dir* **unlink** XDataHub **unlink** XDhuInstall **unlink** XStatus **unlink** XWarn where *app-defaults_dir* is most likely: /opt/SUNWmotif/lib/app-defaults.

10 Remove the DataHub icon from the Xwindows resource file:

From *app-defaults_dir*, edit the Mwm file and remove the DataHub icon lines (normally located at the bottom of the file).

11 Unlink the watchdog command file:

cd /usr/bin
unlink dhu_cmd

12 AIX and Sun only: Remove the NetView launch symbolic links:

cd netview_path/OV/registration/C
unlink datahub.arf
cd netview_path/OV/bin
unlink datahub.lf
cd netview_path/OV/icons/gifs
unlink dhlogo.gif
cd netview_path/OV/icons/drag-bitmaps
unlink dhubnew.xbm

13 Edit the /etc/inittab file and remove the DataHub entries.

> Make a backup copy of the file before editing it; for example:
>
> **cp** /etc/inittab /etc/inittab.bak

14 Start another shell using the user ID of the control database owner:

su - *cdb_owner*

where *cdb_owner* is the user ID.

15 Drop the control database tables and views. Refer to the documentation provided with your database for more information.

16 Exit the shell back to the root session:

exit

17 AIX only: If you installed DataHub using smit and installp, use smit and installp to remove DataHub.

18 Remove the DataHub directory:

rm -R *datahub_path*

Appendix A. DataHub System Modifications

This appendix lists system changes made by the DataHub configuration programs. The dhuinst or dhuinstty programs:

- Optional: Create a symbolic link from your library directory to the IPF/X library, libipfx.a, to access the help files.
- Create a symbolic link from your library directory to the shared library:

AIX	libdhu.o
HP	libdhu.sl
Sun	libdhu.so

- Set a symbolic link from the X Windows System apps-defaults directory to the resource file XDataHub.
- Set a symbolic link from the /usr/bin directory to the /etc/dhu_cmd file.
- Add the DataHub icon to the X Windows System resource file (Mwm) in the apps-defaults directory.
- Set a symbolic link from the /usr/bin directory to the dhtrap file.
- AIX only: Set symbolic links for NetView launch:
  - From the netview_path/OV/registration/C directory to the datahub.arf file
  - From the netview_path/OV/bin directory to the datahub.lf file
  - From the netview_path/OV/icons/gifs directory to the dhlogo.gif file
  - From the netview_path/OV/icons/drag-bitmaps directory to the dhubnew.xbm file
- Put the DataHub script files rc.dhudrv, rc.dhu_gcs, rc.dhu_sms, rc.dhu_ia, dhu_cmd, dhu_klog, and rc.dhuwdg in the /etc directory.
- Create or modify these files:

  datahub_path/*system_dir*/gui/apps.pl
  datahub_path/*system_dir*/gui/dba_install.sql
  datahub_path/*system_dir*/gui/datahub
  datahub_path/*system_dir*/server/config.pl

- Add the DataHub services and socket port numbers to the /etc/services file.
- Add the entry local3.info to the /etc/syslog.conf file.

- Add and populate the necessary tables and views of the control database.
- Update the /etc/inittab file to start DataHub script files automatically when the workstation operating system is started.
- If you selected to do so, start the scripts that drive the DataHub component processes (operating system driver, watchdog server, database driver that corresponds with the RDBMS type of the control database).

Appendix B. Script Files Used by DataHub

There are six key script files in DataHub.

datahub
: Starts the product. This script:

1. Sets and exports various paths
2. Defines application parameters
3. Specifies directories
4. Invokes the DataHub control point application

The datahub script is created during control point configuration and placed in the /gui directory.

rc.dhudrv
: Starts the operating system and database drivers. This script is started (usually) when you configure DataHub. An entry for this script is placed in /etc/inittab during DataHub configuration.

rc.dhu_gcs
: Starts the watchdog server. This script is started (usually) when you configure DataHub. An entry for this script is placed in /etc/inittab during DataHub configuration (on the workstation containing the watchdog server).

rc.dhu_sms
: Starts watchdog evaluation processes. This script is started (usually) when you configure DataHub. An entry for this script is placed in /etc/inittab during DataHub configuration.

rc.dhu_ia
: Starts the control database access processes. This script is started (usually) when you configure DataHub. An entry for this script is placed in /etc/inittab during DataHub configuration (on the workstation containing the watchdog server). This file calls another script file, CDBAccess, which starts communications between the watchdog server and the control database. CDBAccess contains the password used by the watchdog server to access the control database.

rc.dhuwdg
: Starts the operating system and database watchdogs. This script is started (usually) when you configure DataHub. An entry for this script is placed in /etc/inittab during DataHub configuration.

The DataHub configuration programs place the last five script files into /etc/inittab, so they will be started automatically when the workstation is rebooted.

Also, the last five scripts (rc.dhudrv, rc.dhu_gcs, rc.dhu_sms, rc.dhu_ia, and rc.dhu_wdg) are usually started when you configure DataHub. If you ever need to start them manually, start them in the order shown in this appendix. For more information, see “Checking Common DataHub Processes” on page 78.

Appendix C. DataHub Passwords

DataHub accesses data using standard RDBMS methods, including authorization according to user ID and password. Most passwords are provided by the user at the point of initial data access. These passwords are typed into fields presented by the control point application.

There are, however, a few passwords that are stored by DataHub. You might want to protect these passwords by using normal file protection methods. In addition, you might need to change these passwords from time to time, based on your local requirements.

The three password types are described in:

- "Watchdog Server Password"
- "Sybase Watchdog Password"
- "Configuration Passwords"

Watchdog Server Password

The watchdog server requires access to the control database. A user ID and password are required to access the database. The password used by the watchdog server is provided during DataHub configuration and is stored in the *datahub_path*/*system_dir*/server/CDBAccess file. The password is set at the top of the file with the CDBPWD variable. The user ID used by the watchdog server to access the control database is the user specified as the Database Owner during configuration of the control point or the control database.

Sybase Watchdog Password

The Sybase watchdog requires access to the Sybase server. A user ID and password are required to access the Sybase server. The password used by the Sybase watchdog is provided during DataHub configuration and is stored in the rc.dhuwdg file in the /etc directory. A copy of this file is also located in the *datahub_path/system_dir/*gui directory. The Sybase server user and password are stored as the fifth and sixth parameters of the line starting with start_watchdog2.

Configuration Passwords

A few files containing passwords might remain in the datahub_dir/system_dir/install directory. Examples are files ending in .mem and the install.log file. These files should be protected or removed.

Bibliography

This bibliography includes all publications cited in this book; it also lists publications that provide additional information for DataHub users.

The DataHub for UNIX Operating Systems Library

The following books comprise the DataHub for UNIX Operating Systems library:

- *DataHub for UNIX Operating Systems User's Guide*, SC26-8668

  This book describes how to use the DataHub product. It uses a task-oriented approach, describing actions you can take rather than how the product works.

- *DataHub for UNIX Operating Systems Installation and Configuration Guide*, SC26-8669

  This book describes installation, configuration, customization, and trouble-shooting procedures for DataHub.

Related IBM Publications

This section lists books associated with IBM products.

AIX/6000 Publications

- *AIX Version 3.2 for RISC System/6000 Installation Guide*, SC23-2341
- *AIX Version 3.3 for RISC System/6000 Commands Reference*, GBOF-1802
- *AIXwindows Environment/6000 AIXwindows and AIXwindows Desktop User's Guide*, GC23-2432

DB2 for AIX Publications

- *DB2/6000 Administration Guide*, SC09-1571
- *DB2 for AIX Information and Concepts Guide*, S20H-4664
- *DB2 for AIX Administration Guide*, S20H-4580
- *DB2 for AIX Command Reference*, S20H-4645
- *DB2 for AIX API Reference*, S20H-4984
- *DB2 for AIX SQL Reference*, S20H-4665
- *DB2 for AIX Database System Monitor Guide and Reference*, S20H-4871
- *DB2 for AIX Messages Reference*, S20H-4808
- *DB2 for AIX Problem Determination Guide*, S20H-4779
- *DB2 for AIX Planning Guide*, S20H-4758
- *DB2 for AIX Installation and Operation Guide*, S20H-4757
- *DB2 for AIX Master Index and Glossary*, S20H-4781

DB2 for HP-UX Publications

- *DB2 for HP-UX Installation and Operation Guide*, S34H-0898
- *DB2 for HP-UX Planning Guide*, S34H-0897

DB2 for AIX publications listed under "DB2 for AIX Publications" on page 101 (except for S20H-4757 and S20H-4758) apply to DB2 for HP-UX.

DB2 for Solaris Publications

- *DB2 for the Solaris Operating Environment Installation and Operation Guide*, S34H-0893
- *DB2 for the Solaris Operating Environment Planning Guide*, S34H-0892

DB2 for AIX publications listed under "DB2 for AIX Publications" on page 101 (except for S20H-4757 and S20H-4758) apply to DB2 for Solaris.

Publications of Other Companies

This section lists RDBMS books produced by other companies.

INGRES Publications

- *INGRES Database Administrator's Guide (UNIX)*, 64-99-17901
- *INGRES Installation and Operations Guide (UNIX)*, 6-99-#io9-64
- *INGRES Master Index (UNIX)*, 64-99-18902
- *INGRES Object Management User's Guide*, 63-9(9)-47301
- *INGRES/QUEL Command Summary*, 64-9(9)-48106

Oracle Publications

- *ORACLE7 Server Concepts Manual*
- *ORACLE7 PL/SQL User's Guide and Reference*
- *ORACLE7 Messages and Codes Manual*
- *ORACLE7 SQL*Plus User's Guide and Reference*
- *ORACLE7 Server Administrator's Guide*
- *ORACLE7 Server Application Developer's Guide*
- *ORACLE7 Server Utilities User's Guide*

SYBASE SQL Publications

- *SYBASE SQL Server Administration Guide*
- *SYBASE SQL Server Master Index*
- *SYBASE SQL Server Reference Manual*
- *SYBASE SQL Server Troubleshooting Guide*
- *SYBASE SQL Server Utility Programs for UNIX*

- *Transact-SQL User's Guide*
- *Open Client Embedded SQL Reference Manual*

Terms and Abbreviations

This glossary contains information about the terms and abbreviations used in the DataHub for UNIX Operating Systems user interface and publications. Many definitions include additional information about how the term applies when you use DataHub for UNIX Operating Systems.

This list is not exhaustive; you should refer to the manuals for your particular RDBMS for the definitions of database objects particular to that RDBMS.

A

action. A defined task that DataHub performs. An action might be *to display* database activity, *to add* authorizations, or *to run* SQL.

action log. A file on a managed host to which is written watchdog actions and results.

action type. A category of event that occurs when a watchdog rule condition is met. An alert is one action type.

Action window. The left window of the three windows that together make up the DataHub for UNIX Operating Systems *main window*. It contains zero, one, or more action push buttons which represent actions that can be performed on the objects selected in the Object Tree window.

Advanced Interactive Executive (AIX or AIX/6000). IBM's operating system for the RISC System/6000 workstation.

AIX. See *Advanced Interactive Executive.*

AIX/6000. See *Advanced Interactive Executive.*

alert. (1) The screen object, usually containing a text message and a flashing color, sent to a named user in response to a condition reported by a watchdog and evaluated by a watchdog rule. (2) An action type associated with a watchdog rule. When a watchdog rule is defined, part of the definition is the watchdog rule action type. Possible action types include sending an alert, launching a program, and generating an SNMP trap.

See also *watchdog rule* and *watchdog check.*

alias. (1) In DB2, an alternative name used to identify an object or a database. (2) In Sybase, an alternative name used to identify a database user.

authorization. A right granted to a user or group of users to communicate with or make use of a computer system or database.

automated operations. DataHub functions that can take automatic corrective actions for databases and operating systems. The automatic operations occur when a predefined condition or set of conditions is met (defined using watchdog checks and rules). See *offline monitoring.*

B

backup. (1) To copy information onto a diskette, fixed disk, tape, or other storage media for record keeping or recovery purposes. (2) A copy of one or more table spaces or a copy of an entire database at a given point in time. This copy is saved for future reference or for recovery purposes in case the original data is damaged or lost.

C

catalog. See *database catalog.*

cascading pull-down menu. A pull-down menu invoked by selecting an option on another pull-down menu.

check. See *database check* and *watchdog check.*

collapse. (1) To temporarily prune or remove branches of the tree currently displayed in the

DataHub for UNIX Operating Systems Object Tree window. A collapse operation is reversed by selecting **Expand**.

(2) A term relating to the Table of Contents of an online publication. To collapse a topic, you can use the mouse to click on the minus sign beside the topic. The plus sign that appears beside the topic indicates that you can *expand* the topic.

commit. In SQL, the process that allows data changed by one application or user to be used by other applications or users. When a commit operation is complete, the locks are released to allow other applications to use the changed data.

configuration. The process used to set up the DataHub files and environment according to user specifications. This process sets up the control point application, loads the control database, and sets up and starts the watchdog server, driver, and watchdog processes. This process is used on the control point system and the managed hosts. The installation process must be completed prior to starting the configuration process.

container. A generic term describing an allocation of space to a table space. Depending on the table space type, a container can be a directory name, a device name, or a file name.

contextual help. Help that gives information about the specific item the cursor is on.

Contrast with *general help.*

control database. A database containing DataHub for UNIX Operating Systems tables, watchdog rules, watchdog checks, alerts, users, managed systems, and other such information.

control point. The DataHub for UNIX Operating Systems control point is the programmable workstation from which you invoke DataHub functions.

Contrast with *managed host.*

See also *managed database.*

D

daemon. An unattended UNIX process that provides services upon request or periodically. DataHub watchdogs are examples of daemons.

database. A collection of data with a given structure for accepting, storing, and providing data for multiple users on demand.

database administrator (DBA). An individual or group responsible for the design, development, operation, safeguarding, maintenance, and use of a database.

database catalog. A set of system tables maintained by the database manager. Catalog tables are created when the database is created and contain information about database objects such as tables, views, and indexes and their relationships.

database device. A Sybase device for storing the objects that make up databases in a Sybase server.

database driver. A process supporting DataHub database operations.

DataHub provides database drivers for all RDBMSs that it manages. See *DataHub for UNIX Operating Systems* for a list of RDBMSs. See also *driver*.

database watchdog. An unattended process that performs watchdog checks on a managed database at predefined times or time intervals.

DATABASE 2 for AIX (IBM DB2 for AIX). A relational database management system designed for the AIX platform. The major components include database services and facilities to access data, the DBA utility, and application interfaces. DB2 for AIX allows users to create, update, and access databases.

data dictionary. For ORACLE databases, the data dictionary is a set of tables that provides information about its associated database.

DataHub. See *DataHub for UNIX Operating Systems*.

DataHub for UNIX Operating Systems. An IBM product that provides database and system administration and monitoring functions. DataHub for UNIX Operating Systems manages DB2, INGRES, ORACLE, and SYBASE SQL Server databases. DataHub for UNIX Operating Systems operates on and manages AIX, HP-UX, and Sun Solaris.

DataHub group. An object type that appears in the object tree, the occurrences of which represent more than one object. There are group objects for hosts, servers, and databases. See also *group member* and *group object*.

DataHub for UNIX Operating Systems window. The main product window. Composed of three distinct areas: Action window, Object Tree window, and Navigation window. All three windows change dynamically to reflect your selections, available actions, and your navigation path through and current position in the Object Tree window.

DBA. See *database administrator.*

DB2. See *DATABASE 2 for AIX*.

default device. The device chosen by the Sybase system when no device is specified.

delimited identifier. In SQL, a sequence of one or more characters enclosed within quotation marks.

device. In Sybase systems, a disk space or a file in the file system that is used to store databases and their objects.

distributed relational database system. A system involving multiple locations connected together in a communications network, in which each location may have one or more like or unlike relational database systems. In a distributed relational database management system, a user at one location can access any data in the network as if the data were stored at the user's location.

DNS. See *Domain Name Service*.

Domain Name Service. A mechanism, in TCP/IP, that tracks the host names in a network. A domain name consists of a sequence of subnames separated by a delimiter character.

double-byte character set (DBCS). A set of characters in which each character occupies two bytes. Languages, such as Japanese, Chinese, and Korean, that contain more symbols than can be represented by 256 code points require double-byte character sets. Entering, displaying, and printing DBCS characters requires special hardware and software support.

driver. A process supporting DataHub operations on a specific operating system or specific RDBMS. A minimum DataHub configuration requires one operating system driver and one database driver (for the control database). See also *operating system driver* and *database driver*.

dump device. A Sybase device for storing backup copies of databases or transaction logs.

E

entry field. An area of the window where you can type information. Its boundaries are usually indicated. See also *selection field.*

event. An occurrence of significance to a task. In an INGRES RDBMS, an event is any type of a program detectable occurrence.

expand. (1) To display collapsed branches of the object tree currently displayed in the DataHub for UNIX Operating Systems window. A plus (+) symbol inside a circle to the right of a branch indicates that the branch can be expanded.

(2) A term relating to the Table of Contents of an online publication. To expand a topic, click on the plus sign beside the topic.

A minus sign beside a topic indicates that you can *collapse* the topic.

extended help. Help that provides information about the contents of the window from which a user requested help. Contrast with *contextual help*.

F

filter. (1) A value you can specify to limit the objects displayed in the DataHub for UNIX Operating Systems Object Tree window. For example, filters allow you to limit the number of tables that will be displayed on the object tree to those owned by a specific user or those tables with names starting with a specific character string. (2) A value you can specify to establish a threshold for a watchdog check. When the threshold is reached or exceeded, the check results are evaluated by rules. Watchdog filters can help DBAs implement a management-by-exception system.

fire. To initiate the action specified by a rule when the condition stated by the rule is satisfied.

foreign key. A column or set of columns in a table whose values are required to match at least one primary key value of a row of its parent table.

function. A program or piece of a program that can be called. For DB2, a function represents a specific purpose of an entity or its characteristic action, such as a column function or a scalar function. For ORACLE, a function is a PL/SQL block that contains procedural constructs and embedded SQL statements that can have input arguments only.

G

general help. In DataHub, a help panel providing general information about the DataHub for UNIX Operating Systems window. This panel is invoked from the Help menu.

Contrast with *contextual help* and *extended help*.

global rules evaluation. The analysis of monitoring results from resources on multiple hosts for cross-system problems. See *watchdog server*.

graying. An indication that a choice is unavailable.

group. (1) A logical organization of users that have IDs according to activity or resource access authority. (2) DataHub group.

group member. A member of a DataHub group, such as a host, server, or database. Group members can be displayed in the object tree below the group to which they belong. See also *DataHub group*.

group object. DataHub groups can have group objects that represent an object that is common to all of the members of the group. Group objects are displayed in the object tree below the group to which they belong. For example, a database group could have group users, group table spaces, and group tables. See also *DataHub group*.

guard. An optional component of the rule text for a watchdog rule that determines whether the condition is evaluated.

GUI. graphical user interface.

H

heterogeneous environment. A computing environment composed of differing hardware and software components typically supplied by multiple vendors. DataHub works across different UNIX systems and controls RDBMSs from various database vendors.

hide. To remove objects and branches of objects from the Object Tree window. Objects are not actually removed from the system or RDBMS; Hide merely removes objects from the Object Tree window.

host. A local or remote workstation running a DataHub-supported operating system. DataHub manages host operating systems and host RDBMSs.

HP-UX. Hewlett-Packard operating system for UNIX workstations

I

identifier. One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element.

index. A set of row pointers that are logically ordered by the values of a key. Indexes provide quick access to data and can enforce uniqueness on the rows in the table.

index key. A column or an ordered collection of columns on which an index is defined. See also *key*.

installation. The process used to copy DataHub files from the install media to the DataHub directories on the control point and managed hosts.

instance. A logical database manager environment similar to an image of the actual database manager environment.

intelligent agent. See *watchdog*.

J

join. A relational operation that allows for retrieval of data from two or more tables based on matching column values.

join condition. A condition where two tables are brought together and compared; rows from one table are selected when columns from that table match columns (over a condition) from the other table.

journal. A file used to record changes made in a system. Synonymous with *log*.

K

key. A column or an ordered collection of columns that uniquely identifies a row.

L

LAN. See *local area network.*

launch. The initiation of an executable program, shell script, or command. A launch is one of the three options you can specify in a watchdog rule as the action to be taken if the conditions specified in the watchdog rule are met.

local area network (LAN). A network of devices that are connected to one another for communication. A local area network can be connected to another LAN or to a larger network (wide area network or WAN). See also *wide area network*.

local rules evaluation. Analysis of monitoring results from a specific managed host done at that host.

log. (1) To record; for example, to log all messages on the system printer. (2) See *journal*, *action log*.

login. In a Sybase RDBMS, the name used to log in to a SQL Server.

M

managed database. A database defined to the DataHub control point. The DataHub control point always has at least one managed database (the control database).

managed host. An operating system that is defined to the DataHub control point.

managed system. See *managed host*.

management by exception. See *filter*.

menu bar. The rectangular area at the top of the DataHub for UNIX Operating Systems window containing headings for pull-down menus. The headings, called menu choices, are File, Tree, Options, Administer, and Help. Click on menu choices to access pull-down menus. For example, when you select **Help** on the menu bar, the **Help** pull-down menu is displayed.

N

Navigation window. The window on the right side of DataHub for UNIX Operating Systems window, showing the path you travelled in the Object Tree window.

O

object class. See *object type*.

object instance. See *object occurrence*.

object occurrence. An element of the environment managed by DataHub. Each named object under an object type (host, database, package, and so on) is an occurrence of that object. In DataHub, an example of an object occurrence might be a relational database named CELDIAL that appears under the Database object type in the DataHub for UNIX Operating Systems Object Tree window.

Object Tree window. The window in the middle of the DataHub for UNIX Operating Systems window. The Object Tree window contains a list of managed object types and object occurrences within the DataHub for UNIX Operating Systems window.

The objects in the DataHub for UNIX Operating Systems window are displayed in a tree formation. The tree structure shows relationships between hosts, databases, and related database objects. Objects are shown in a hierarchical list with connecting lines between associated objects.

object type. DataHub grouping term for a stored collection of elements with the same definition. An object type (host, database, user, and so on) groups named occurrences of that type.

occurrence. See *object occurrence.*

offline monitoring. The DataHub monitoring capabilities that use watchdogs. DataHub watchdog checks monitor operating systems and RDBMSs without user intervention. Monitoring results can be filtered so only exception conditions are reported.

Contrast with *online monitoring*.

See also *watchdog check* and *watchdog rule*.

online monitoring. Direct, user-initiated monitoring operations started from the DataHub for UNIX Operating Systems window. Examples of online monitoring are displaying file system and CPU usage, disk I/O, and processes.

operating system driver. A required process supporting DataHub operations on UNIX operating systems. There is one operating system driver for each operating system managed from a DataHub for UNIX Operating Systems control point.

DataHub for UNIX Operating Systems provides operating system drivers for AIX, HP-UX, and Sun Solaris systems.

operating system watchdog. An unattended process that performs watchdog checks on a managed host at predefined times or time intervals.

ordinary identifier. In SQL, a letter, which might be followed by zero or more characters, each of which is a letter (a-z and A-Z), a symbol, a number, or the underscore character, used to form a name.

out-of-the-box monitoring. A subset of the DataHub predefined checks, with associated filter values and rules, that can be activated as a unit whenever a host, Sybase server or database is added or its definition modified. The filters represent typical exception conditions, and the rules offer advice to the DataHub administrator for dealing with the detected situation.

P

package. The control structure produced when the SQL statements in an application program are bound to a RDBMS. The RDBMS uses the control structure to process SQL statements encountered during statement execution.

predefined check. A watchdog check that is available for selection when you create a new check. Check commands and return types are provided in predefined checks. See also *watchdog check*.

primary key. A column or an ordered set of columns that contain non-null values and whose values uniquely identify a row. A table cannot have more than one primary key.

privilege. The right or authority to access a specific database object in a specific way.

prompt. A symbol or action that requests you to enter information.

pull-down menu. A list of choices extending from a selected menu choice that gives you access to actions, routings, and settings.

push button. A small, selectable rectangle with text inside used in program windows to start actions. Examples of push buttons are the **Display** push button and the **OK** push button.

Q

quiesce. To bring a device or system to a halt by rejecting new requests for work.

quoted name. An identifier enclosed in double quotes.

R

radio button. A diamond with text beside it. Radio buttons come in multiples to show a fixed set of choices from which only one can be selected. The diamond is partially filled when a choice is selected.

RDB. See *relational database.*

RDBMS. See *relational database management system.*

referential constraint. The relationship between two tables that controls the association between them, ensuring data consistency.

recovery. (1) The act of resetting a system, or data stored in a system, to an operable state following damage. (2) The process of rebuilding databases by restoring a backup copy and rolling forward the logs associated with it.

relational database (RDB). A database in which the data is organized and accessed according to relations.

relational database management system (RDBMS). A system that manages relational databases. DataHub for UNIX Operating Systems supports the following RDBMSs:

- DB2 Version 1
- DB2 Version 2
- INGRES
- ORACLE
- SYBASE SQL Server

restore. To return a backup copy to active storage for use.

roll-forward. To update the data in a restored database by applying changes recorded in the logs of transactions in the database.

root object. (1) In the UNIX operating system, the user name for the system user with the most authority. (2)An icon at the top of the object tree. The root icon is selected to display object types such as hosts, servers, and DataHub groups.

rule. See *watchdog rule*.

S

scroll bar. A part of a window, associated with a scrollable area, that a user interacts with to see information that is not currently visible. Scroll bars allow scrolling up and down, and left and right.

select. To identify one or more object types or occurrences to which a subsequent action should apply. An object can be selected by moving the cursor to the item and clicking mouse button 1.

selection field. An area of a window that contains a fixed number of choices from which the user can select. See also *entry field.*

selection list. A list of choices that a user can scroll through to select a choice.

self-join. To join a table or view with itself. See also *join*.

shell procedure. See *shell script*.

shell script. A series of commands combined in a file that carries out a particular function when the file is run or when the file is specified as a value to the **sh** command. Synonymous with shell procedure.

SNMP. Simple Network Management Protocol

Solaris. Sun Microsystems Solaris operating system for UNIX workstations.

SQL. See *Structured Query Language.*

Structured Query Language (SQL). A language that can be used within programs or interactively to define database objects, manipulate data, and control access to resources in a relational database environment.

stored procedure. A block of procedural constructs and embedded SQL statements that is stored in a database and can be called by name.

T

table. A named data object consisting of a specific number of columns and some unordered rows.

table column. A vertical component of a table that consists of a name, a particular data type, and, if necessary, a length. All values in a particular column share this same data type.

table space. In DB2 Version 2, a pageset that is used to store the records of one or more tables and, optionally, indexes.

tablespace. In ORACLE, a logical storage unit into which a database is divided.

TCP/IP. See *Transmission Control Protocol/Internet Protocol.*

threshold. A value that can be specified for a watchdog check. When the result of a watchdog check meets or exceeds this threshold value, the rule associated with this check is evaluated. See also *filter*.

token-ring address. A unique 12-digit number that identifies a system′s location within a token-ring network.

toggle button. A small window object providing binary selection (such as on or off) for a process option in a window.

transaction log. A system table in which all changes to the database are recorded.

Transmission Control Protocol/Internet Protocol (TCP/IP). Part of the internet suite of protocols that allows users to communicate with each other in a consistent way regardless of the technology implemented in each node across the network.

trigger. Defines an action to be executed when a given update operation (DELETE, INSERT, or UPDATE) occurs for a specified table.

U

user directory. A directory in the UNIX operating system where user files and other directories are typically stored. The conventional names for these directories are: /u for AIX, /usr for HP-UX, and /opt for Sun Solaris.

user ID. A string of characters that identifies a user to a system (RDBMS or managed host system.)

user password set. An object in the object tree that represents a user ID and password for DataHub group objects. A user password set links the user ID and password for each group member to the user ID and password for a whole group.

W

WAN. See *wide area network.*

watchdog. A process providing *offline monitoring* capabilities. A watchdog is also referred to as an intelligent agent. Watchdogs are specific to run-time environments (operating systems and RDBMSs). For example: an AIX operating system is monitored by an operating system watchdog specific to AIX; an ORACLE database is monitored by an ORACLE watchdog. Each system and RDBMS to be monitored requires a watchdog. For example, if there are two occurrences of DB2 for AIX and one occurrence of an ORACLE RDBMS on a managed host, and all RDBMSs are to be monitored, you must have two DB2 for AIX watchdogs and one ORACLE watchdog running on that managed host.

Initially from the global rules evaluator, and then from the monitoring system on the managed host, watchdogs receive conditions to monitor (watchdog checks), filter values, watchdog check times, and instructions on whether or not to store check values. Results (watchdog values) are returned to the monitoring system for evaluation by watchdog rules.

watchdog check. An operating system command, SQL statement, or shell script run at predefined times. Watchdog checks are executed by watchdog processes. Any number of watchdog checks can be defined for each active watchdog. A watchdog check must return a single value that is an integer, floating point number, or string. Filtered values can be stored in the control database.

The values produced by executing watchdog checks are evaluated by watchdog rules.

See also *alert*, *filter*, *watchdog*, *watchdog rule*, and *watchdog server*.

watchdog rule. A condition or set of conditions for values returned by one or more watchdog checks. Watchdog rules define acceptable limits for the condition or conditions and specify an action to be taken if the conditions are met.

watchdog server. The watchdog server performs global rule evaluation. It sends watchdog checks, filter values, and watchdog check times to watchdogs. It receives watchdog check values from the watchdogs when rule evaluation requires input from two or more managed hosts. If the watchdog server evaluates a rule, it determines whether an action is required and what action to take. The action can include sending an alert or launching an executable.

wide area network. A network of devices that are connected to one another for communication over a large distance.

window. An area of the GUI with visible boundaries within which information is displayed. A window can be smaller than, or the same size as, the screen on the display device.

X

X client. Hardware-independent process that requests input/output from an X server.

X server. An application that controls the basic windowing mechanism used for input and output on X Window System displays.

X Window System. The window management and drawing management standard for UNIX operating systems. The X Window System consists of an X server, which manages a visual display, and client application programs.

Index

Special Characters

A

B

C

E

F

M

N

O

P

We′d Like to Hear from You

DataHub for UNIX Operating Systems
Installation and Configuration Guide
Release 2

Publication No. SC26-8669-01

Please use one of the following ways to send us your comments about this book:

- Mail—Use the Readers′ Comments form on the next page. If you are sending the form from a country other than the United States, give it to your local IBM branch office or IBM representative for mailing.
- Fax—Use the Readers′ Comments form on the next page and fax it to this U.S. number: 408-463-4393.
- Internet: COMMENTS@VNET.IBM.COM

  Be sure to include the following with your comments:

  - Title and publication number of this book
  - Your name, address, and telephone number if you would like a reply

Your comments should pertain only to the information in this book and the way the information is presented. To request additional publications, or to comment on other IBM information or the function of IBM products, please give your comments to your IBM representative or to your IBM authorized remarketer.

IBM may use or distribute your comments without obligation.

Readers′ Comments

DataHub for UNIX Operating Systems
Installation and Configuration Guide
Release 2

Publication No. SC26-8669-01

How satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Technically accurate	•	•	•	•	•
Complete	•	•	•	•	•
Easy to find	•	•	•	•	•
Easy to understand	•	•	•	•	•
Well organized	•	•	•	•	•
Applicable to your tasks	•	•	•	•	•
Grammatically correct and consistent	•	•	•	•	•
Graphically well designed	•	•	•	•	•
Overall satisfaction	•	•	•	•	•

Please tell us how we can improve this book:

May we contact you to discuss your comments? • Yes • No

Name

Address

Company or Organization

Phone No.

Readers' Comments
SC26-8669-01

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Department J58
P.O. Box 49023
San Jose CA 95161-9945

Fold and Tape | **Please do not staple** | Fold and Tape

SC26-8669-01

Cut or Fold
Along Line

Part Number: 33H5132
Program Number: 5765-530

Printed in U.S.A.

33H5132

SC26-8669-01

DSMPSP544E PAGE SEGMENT 7X9BOXF PSEG38PP NOT FOUND.
DSMMOM395I '.EDFAWRK' LINE 920: .si 7x9boxf inline
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 2330 OF '.EDF#CV'
DSMMOM397I '.EDF#CV' WAS IMBEDDED AT LINE 120 OF '.EDF#FCV5'
DSMMOM397I '.EDF#FCV5' WAS IMBEDDED AT LINE 330 OF '.EDFCOVER'
DSMMOM397I '.EDFCOVER' WAS IMBEDDED AT LINE 48 OF 'DHUI3MST'
DSMBEG323I STARTING PASS 2 OF 3.
DSMPSP544E PAGE SEGMENT 7X9BOXF PSEG38PP NOT FOUND.
DSMMOM395I '.EDFAWRK' LINE 920: .si 7x9boxf inline
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 2330 OF '.EDF#CV'
DSMMOM397I '.EDF#CV' WAS IMBEDDED AT LINE 120 OF '.EDF#FCV5'
DSMMOM397I '.EDF#FCV5' WAS IMBEDDED AT LINE 330 OF '.EDFCOVER'
DSMMOM397I '.EDFCOVER' WAS IMBEDDED AT LINE 48 OF 'DHUI3MST'
DSMBEG323I STARTING PASS 3 OF 3.
DSMPSP544E PAGE SEGMENT 7X9BOXF PSEG38PP NOT FOUND.
DSMMOM395I '.EDFAWRK' LINE 920: .si 7x9boxf inline
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 2330 OF '.EDF#CV'
DSMMOM397I '.EDF#CV' WAS IMBEDDED AT LINE 120 OF '.EDF#FCV5'
DSMMOM397I '.EDF#FCV5' WAS IMBEDDED AT LINE 330 OF '.EDFCOVER'
DSMMOM397I '.EDFCOVER' WAS IMBEDDED AT LINE 48 OF 'DHUI3MST'