Contacting BMC Software

Several methods are available for contacting BMC Software.

You can access the BMC Software website at http://www.bmc.com. From this website, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

United States and Canada

<table>
<thead>
<tr>
<th>Address</th>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC SOFTWARE INC</td>
<td>1 713 918 8800</td>
<td>1 713 918 8000</td>
</tr>
<tr>
<td>2103 CITYWEST BLVD</td>
<td>or</td>
<td>or</td>
</tr>
<tr>
<td>HOUSTON TX 77042-2827 USA</td>
<td>1 800 841 2031</td>
<td>1 800 841 2031</td>
</tr>
</tbody>
</table>

Outside United States and Canada

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>+01 713 918 8800</td>
<td>+01 713 918 8000</td>
</tr>
</tbody>
</table>

© Copyright 2012-2016 BMC Software, Inc.

BMC, BMC Software, the BMC logo, the BMC Software logo, and other BMC marks are the exclusive properties of BMC Software, Inc. and are registered or may be registered in the U.S. and in other countries. BladeLogic and other BladeLogic marks are the exclusive properties of BladeLogic, Inc. and are registered or may be registered in the U.S. and in other countries. All other trademarks or registered trademarks are the property of their respective owners.

DCE and Explorer are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

DB2, FlashCopy, IBM, IBM z, IMS, MVS, OS/390, Parallel Sysplex, RACF, VTAM, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

SAP is a trademark or registered trademark of SAP AG in Germany and in several other countries.

UNIX is the registered trademark of The Open Group in the US and other countries.

The information included in this documentation is the proprietary and confidential information of BMC Software, Inc., its affiliates, or licensors. Your use of this information is subject to the terms and conditions of the applicable End User License agreement for the product and to the proprietary and restricted rights notices included in the product documentation.

Restricted rights legend

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED—RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC SOFTWARE INC, 2103 CITYWEST BLVD, HOUSTON TX 77042-2827, USA. Any contract notices should be sent to this address.
**Customer support**

**Support website**

You can obtain technical support from BMC 24 hours a day, 7 days a week at [http://www.bmc.com/support](http://www.bmc.com/support). From this website, you can:

- Read overviews about support services and programs that BMC offers
- Find the most current information about BMC products
- Search a database for problems similar to yours and possible solutions
- Order or download product documentation
- Download products and maintenance
- Report a problem or ask a question
- Subscribe to receive proactive e-mail alerts
- Find worldwide BMC support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

**Support by telephone or e-mail**

In the United States and Canada, if you need technical support and do not have access to the web, call 1 800 537 1813 or send an e-mail message to [customer_support@bmc.com](mailto:customer_support@bmc.com). (In the subject line, enter **SupID:** your**SupportContractID**, such as SupID:12345). Outside the United States and Canada, contact your local support center for assistance.

**Before contacting BMC**

Have the following information available so that Customer Support can begin working on your issue immediately:

- **Product information**
  - Product name
  - Product version (release number)
  - License number and password (trial or permanent)
- **Operating system and environment information**
  - Machine type
  - Operating system type, version, and service pack or other maintenance level such as PUT or PTF
  - System hardware configuration
  - Serial numbers
  - Related software (database, application, and communication) including type, version, and service pack or maintenance level
- **Sequence of events leading to the problem**
- **Commands and options that you used**
- **Messages received (and the time and date that you received them)**
  - Product error messages
  - Messages from the operating system
  - Messages from related software
License key and password information

If you have questions about your license key or password, contact Customer Support through one of the following methods:

- Send an e-mail message to customer_support@bmc.com. (In the Subject line, enter `SupID:yourSupportContractID`, such as SupID:12345.)
- In the United States and Canada, call 1 800 537 1813. Outside the United States and Canada, contact your local support center for assistance.
## Contents

### About this book
- Conventions ................................................................. 11
- Syntax diagrams ............................................................. 11
- Related publications ..................................................... 13

### Chapter 1  Overview of customization tasks
- BMC High Speed Utilities for DB2 customization tasks .................................................. 15
- BMC Object Administration for DB2 customization tasks ............................................. 18
- BMC Performance for DB2 SQL customization tasks .................................................... 25
- BMC Performance for DB2 Databases customization tasks .......................................... 30
- BMC Recovery for DB2 customization tasks ................................................................. 34
- NGT Database Administration for DB2 customization tasks ......................................... 38
- NGT Database Performance for DB2 customization tasks ........................................... 44
- BMC Administrative Assistant for DB2 customization tasks ....................................... 46
- BMC Database Administration for DB2 customization tasks ....................................... 50
- Database Performance for DB2 customization tasks .................................................... 55
- BMC Recovery Management for DB2 customization tasks ......................................... 58
- Administrative products for DB2 customization tasks ................................................... 61
- Backup and Recovery products for DB2 customization tasks ....................................... 66
- Utility products for DB2 customization tasks .................................................................. 69
- NGT utility products customization tasks ....................................................................... 71
- System and SQL Performance products for DB2 customization tasks ......................... 71
- EXTENDED BUFFER MANAGER for DB2 (XBM) and SNAPSHOT UPGRADE FEATURE for DB2 (SUF) customization tasks .................................................. 78

### Chapter 2  Authorizations and security
- Authorization verification ................................................ 81
- User authorizations .......................................................... 82
  - Authorization verification mechanisms for the Backup and Recovery products and Utility products .......................................................... 82
  - Granting user authorizations for the Utility products .................................................. 82
  - NGT Copy user authorizations .................................................................................. 93
  - RECOVERY MANAGER for DB2 user authorizations .............................................. 95
  - NGT Recover user authorizations ............................................................................. 97
  - DASD MANAGER PLUS authorizations .................................................................. 98
  - Configuring security for BMC Workbench ............................................................... 101
Controlling access to the System and SQL Performance products for DB2 ..103
Log Master for DB2 user authorizations ......................................................... 114
PACLOG for DB2 user authorizations ............................................................. 116
R+/CHANGE ACCUM for DB2 user authorizations ................................... 118
Granting user authorizations for EXTENDED BUFFER MANAGER .......... 120
High-speed Apply Engine user authorizations ............................................ 128
NGT data set access and security settings .................................................... 136
NGT authorizations ...................................................................................... 138
Restricting access to the worklist parallelism feature .................................. 140

Chapter 3         System-level changes 143
Setting the MEMLIMIT system parameter .................................................... 143
Modifying installation options after customization ....................................... 146
  Modifying installation options modules ..................................................... 146
Increasing the size of DB2 active logs for LOADPLUS .................................. 148
Customizing products that prevent x37 abends in LOADPLUS .................... 148

Chapter 4         Enabling interactions between products 151
Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products) ...................................................... 151
Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products) .................................................. 153
Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products) ................................................. 154
DASD MANAGER PLUS use within other products ........................................ 156
  Enabling the use of DASD MANAGER PLUS within ALTER or CHANGE MANAGER ............................................................. 156
  Enabling the use of DASD MANAGER PLUS within CATALOG MANAGER .................................................................................. 158
Enabling interaction between RECOVERY MANAGER and other products ............................... 160
  Enabling interaction between RECOVERY MANAGER and Log Master .... 160
  Enabling interaction between RECOVERY MANAGER and NGT Recover .................................................................................. 160
  Enabling interaction between NGT Copy and RECOVERY MANAGER .... 161
  Enabling interaction between RECOVERY MANAGER and PACLOG ...... 161
Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER ........ 161

Chapter 5         Customizing Administrative products 163
Specific ALTER and CATALOG MANAGER customization tasks ................ 163
Creating indexes to improve performance .................................................. 163
Shared components ...................................................................................... 163
Chapter 6  Customizing Backup and Recovery  .................................................. 221

Customizing RECOVERY MANAGER ................................................................. 221
- Required temporary tables for RECOVERY MANAGER ............................... 221
- Preparing for archive logs greater than 64 KB tracks ................................. 222
- Setting up data sharing for RECOVERY MANAGER for DB2 .................. 222
- RECOVERY MANAGER, LGC, and DBC ....................................................... 223
- RECOVERY MANAGER for DB2 archive history file ................................ 223
- RECOVERY MANAGER for DB2 option set ............................................... 224
- RECOVERY MANAGER for DB2 packages ................................................. 224
- RECOVERY MANAGER for DB2 repository .............................................. 224

BCSS commands for PACLOG .......................................................................... 225

Chapter 7  Customizing System and SQL Performance ............................................. 227

Overview ........................................................................................................ 227

Post-installation tasks ..................................................................................... 228
- Defining a DOMPLEX .................................................................................. 229
- Editing the DOMPLEX option set online .................................................. 230
- Verifying the product for data sharing members ....................................... 233
- Customizing the CLISTs for SQL Explorer and CATALOG MANAGER ... 234
- Creating indexes to improve performance ................................................. 236
- Generating Help text from DB2 trace record field descriptions ................ 237
- Editing or reviewing the DBC JCL procedure ............................................. 237
- Adding or replacing the CLIST member for the ISPF interface ............. 240
- Making products available from a menu .................................................. 243
- Invoking SQL Explorer directly .................................................................. 244
- Invoking System and SQL Performance products without LIBDEFs ........ 244
- Verifying or changing the global resource enqueues ............................... 246
- Refreshing the MVS Linklist Lookaside ..................................................... 246
- Verifying the product authorization ........................................................... 246

Customizing the System and SQL Performance products ................................ 247
- Verifying or customizing the DOMPLEX option set .................................. 247
- Verifying or changing DOMPLEX parameters ........................................ 262
- Checking the default User Profile .............................................................. 266
- Additional information about archiving and the NGL .............................. 269

Customizing the OPERTUNE for DB2 product ................................................. 271
- Copying the OPERTUNE procedure to a PROCLIB .................................. 271
- Invoking the OPERTUNE CLIST or the common BMCDISPN panel ....... 273
- Creating an OPERTUNE system profile ................................................... 274
- Defining security for OPERTUNE ............................................................. 275
Chapter 12        Verifying installation  327
Verifying the Administrative products’ installation ................................................... 327
Verifying Backup and Recovery product and Utility product installation .......... 328
Verifying the installation of System and SQL Performance products ................. 329
  Starting the DBC subsystem ................................................................................. 330
  Checking the system console log messages ....................................................... 331
  Starting a product session ..................................................................................... 335
  Selecting a DOMPLEX .......................................................................................... 335
  Issuing a dynamic Explain command ................................................................. 336
  Accessing the Index Component reports ........................................................... 340
  Verifying the SQL Explorer installation ............................................................. 342
  Starting a Pool Advisor or System Performance reporting session .......... 349
Verifying the installation of NGT products ............................................................ 349
  Editing allocation automation .............................................................................. 350

Appendix A        Migrating to a different version of DB2  353
Supported DB2 versions and modes ........................................................................ 353
New DB2 version migration .......................................................................................... 355
  Administrative products and solutions ................................................................. 355
  Backup and Recovery and Utility products and solutions .................................... 361
  System and SQL Performance products and solutions ........................................ 361
Earlier DB2 version fallback ...................................................................................... 363
  Administrative products and solutions ................................................................. 363
  Backup and Recovery products and solutions .................................................... 365
  Utility products ...................................................................................................... 365
  System and SQL Performance products and solutions ........................................ 365
About this book

This book contains detailed information about the associated product or products. This preface explains the special conventions that the book uses, and how to access related publications.

If applicable, the preface also summarizes the major changes included in the latest release of the product.

Conventions

This document uses the following special conventions:

- All syntax, operating system terms, and literal examples are presented in this typeface.

- Variable text in path names, system messages, or syntax is displayed in italic text: 
  
  \textit{testsys/instance/file\texttt{Name}}

- Menu sequences use a symbol to convey the sequence. For example, Actions => Create Test instructs you to choose the Create Test command from the Actions menu.

Syntax diagrams

The following figure shows the standard format for syntax diagrams:
The following example illustrates the syntax for a hypothetical DELETE statement. Because the FROM keyword, alias variable, and WHERE clause are optional, they appear below the main command line. In contrast, the tableName variable appears on the command line because the table name is required. If the statement includes a WHERE clause, the clause must contain a search condition or a CURRENT OF clause. (The searchCondition variable appears on the main line for the WHERE clause, indicating that this choice is required.)

The following guidelines provide additional information about syntax diagrams:

- Read diagrams from left to right and from top to bottom.
- A recursive (left-pointing) arrow above a stack indicates that you may choose more than one item in the stack.
- An underlined item is a default option.
- If a diagram shows punctuation marks, parentheses, or similar symbols, you must enter them as part of the syntax.
- In general, IBM commands, keywords, clauses, and data types are displayed in uppercase letters. However, if an item can be shortened, the minimum required
portion might be shown in uppercase letters, with the remainder in lowercase (for example, CANcel).

- The following conventions apply to variables in syntax diagrams:
  - Variables are typically displayed in lowercase letters and are always italicized.
  - If a variable is represented by two or more words, initial capitals distinguish the second and subsequent words (for example, databaseName).

**Related publications**

From the BMC Support Central website, you can use the following methods to access related publications that support your product or solution:


- View Quick Course videos (short overviews of selected product concepts, tasks, or features), which are available from the following locations:
  - Documentation Center (primary center and secured center)
  - Support Central (at http://www.bmc.com/support/mainframe-demonstrations)
  - BMC Mainframe YouTube channel (https://www.youtube.com/user/BMCSoftwareMainframe)


Products with online interfaces also offer online Help via the F1 key or, for graphical user interfaces (GUIs), via a Help button.

*Tip*

If you prefer hardcopy documentation, you can order it from your BMC sales representative or from Support Central. Also, from Support Central you can subscribe to receive proactive e-mail alerts when BMC issues notices.
Overview of customization tasks

This chapter lists the mandatory and optional customization tasks for each solution and product. You perform these tasks outside the Installation System.

BMC High Speed Utilities for DB2 customization tasks

After you install and configure the BMC High Speed Utilities for DB2 solution, you might need to perform several additional customization tasks to complete and verify the installation. You perform these tasks outside the Installation System dialog panels.

This solution includes the following products or components:

- BMC Next Generation Technology Check for DB2 for z/OS
- CHECK PLUS for DB2
- BMC Next Generation Technology Stats for DB2 for z/OS
- BMC Common Statistics
- BMC Next Generation Technology Copy for DB2 for z/OS
- BMC Next Generation Technology Load for DB2 for z/OS
- LOADPLUS for DB2
- BMC Next Generation Technology Recover for DB2 for z/OS
- BMC Next Generation Technology Reorg for DB2 for z/OS
- REORG PLUS for DB2
- SNAPSHOT UPGRADE FEATURE for DB2 (SUF), which is a component of EXTENDED BUFFER MANAGER for DB2 (XBM)
- BMC Next Generation Technology Unload for DB2 for z/OS
- UNLOAD PLUS for DB2
- BMC Workbench for DB2

Perform the following customization tasks for the BMC High Speed Utilities for DB2 solution, in the order listed.
Table 1: Summary of BMC High Speed Utilities customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
<tr>
<td>Controlling access and setting user authorizations</td>
<td>Use the following information to set the required authorizations for the products in this solution:</td>
</tr>
<tr>
<td></td>
<td>■ “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82</td>
</tr>
<tr>
<td></td>
<td>■ “Setting CHECK PLUS authorizations” on page 82</td>
</tr>
<tr>
<td></td>
<td>■ “NGT Copy user authorizations” on page 93</td>
</tr>
<tr>
<td></td>
<td>■ “Setting LOADPLUS authorizations” on page 84</td>
</tr>
<tr>
<td></td>
<td>■ “NGT Recover user authorizations” on page 97</td>
</tr>
<tr>
<td></td>
<td>■ “Setting REORG PLUS authorizations” on page 88</td>
</tr>
<tr>
<td></td>
<td>■ “Setting UNLOAD PLUS authorizations” on page 91</td>
</tr>
<tr>
<td></td>
<td>■ “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120</td>
</tr>
<tr>
<td></td>
<td>■ “NGT authorizations” on page 138</td>
</tr>
<tr>
<td></td>
<td>■ “Configuring security for BMC Workbench” on page 101</td>
</tr>
<tr>
<td>Completing tasks specific to LOADPLUS</td>
<td>See Table 2 on page 17.</td>
</tr>
<tr>
<td>Completing tasks specific to XBM and SUF</td>
<td>See Table 3 on page 17.</td>
</tr>
<tr>
<td>Completing tasks specific to BMC Workbench</td>
<td>See Table 5 on page 17.</td>
</tr>
<tr>
<td>Completing tasks specific to NGT Check, NGT Load, NGT Reorg, NGT Stats, and NGT Unload</td>
<td>See Table 4 on page 17.</td>
</tr>
</tbody>
</table>

The following tables list additional customization tasks that apply to specific products or components within the solution.
### Table 2: Customization tasks specific to LOADPLUS

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing products that prevent x37 abends in LOADPLUS</td>
<td>See “Customizing products that prevent x37 abends in LOADPLUS” on page 148.</td>
</tr>
<tr>
<td>Increasing the size of DB2 active logs for LOADPLUS</td>
<td>See “Increasing the size of DB2 active logs for LOADPLUS” on page 148.</td>
</tr>
</tbody>
</table>

### Table 3: Customization tasks specific to XBM and SUF

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing XBM subsystems</td>
<td>See “Customizing XBM subsystems” on page 279.</td>
</tr>
<tr>
<td>Customizing XBM components</td>
<td>See “Customizing XBM components” on page 289.</td>
</tr>
</tbody>
</table>

### Table 4: Customization tasks specific to NGT utilities

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up data set access and security settings</td>
<td>See “NGT data set access and security settings” on page 136.</td>
</tr>
<tr>
<td>Setting up NGT authorizations</td>
<td>See “NGT authorizations” on page 138.</td>
</tr>
<tr>
<td>Setting up checkpoints</td>
<td>See “Checkpoint data set considerations” on page 307.</td>
</tr>
<tr>
<td>Configuring block sizes</td>
<td>See “Block size considerations” on page 308.</td>
</tr>
<tr>
<td>Specifying the global utility parameters</td>
<td>See the <em>BMC Next Generation Technology General User Guide</em>.</td>
</tr>
<tr>
<td>Specifying product-specific parameters</td>
<td>See the &quot;Parameters&quot; chapter of the reference manual for each product.</td>
</tr>
<tr>
<td>Setting up the NGT Utility Manager</td>
<td>See the <em>BMC Next Generation Technology Utility Manager for DB2 for z/OS Reference Manual</em>.</td>
</tr>
<tr>
<td>Starting the NGT Subsystem</td>
<td>See “Starting NGT Subsystem” on page 308. For more information, see the <em>BMC Next Generation Technology Subsystem Reference Manual</em>.</td>
</tr>
</tbody>
</table>

### Table 5: Customization tasks specific to BMC Workbench

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading the customization overview</td>
<td>This section provides important background information about customizing BMC Workbench. See “Customization overview” on page 293.</td>
</tr>
</tbody>
</table>
Customization task | Description and link
--- | ---
**Installing SYSPROC.ADMIN_COMMAND_DSN** | If you have not installed SYSPROC.ADMIN_COMMAND_DSN, then perform this task. See “BMC Workbench for DB2 requirements” on page 294.

*(optional) Editing the BMC Workbench option set* | The installation process automatically creates a default option set named GUDOPT that is based on definitions that you supply during installation. If required, you can edit this option set. See “Editing the BMC Workbench option set” on page 298.

**Customizing Common Explain** | Customize Common Explain for use with BMC Workbench. See “Common Explain” on page 300.

---

**BMC Object Administration for DB2 customization tasks**

After you install and configure the BMC Object Administration for DB2 solution, you might need to perform several additional customization tasks to complete and verify the installation. You perform these tasks outside the Installation System dialog panels.

This solution includes the following products or components:

- BMC Common Statistics
- CHANGE MANAGER for DB2
- CATALOG MANAGER for DB2
- BMC Next Generation Technology Copy for DB2 for z/OS
- LOADPLUS for DB2
- BMC Next Generation Technology Load for DB2 for z/OS
- BMC Next Generation Technology Recover for DB2 for z/OS (partial functionality)
- SNAPSHOT UPGRADE FEATURE for DB2 (SUF), which is a component of EXTENDED BUFFER MANAGER for DB2 (XBM)
- UNLOAD PLUS for DB2
- BMC Next Generation TechnologyUnload for DB2 for z/OS
- BMC Workbench for DB2

Perform the following customization tasks for the BMC Object Administration for DB2 solution, in the order listed.
<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying authorization</td>
<td>Verify that your BMC Authorization passwords are saved and copied to the correct library. See “Authorization verification” on page 81.</td>
</tr>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
</tbody>
</table>
| Controlling access and setting user authorizations | Use the following information to set the required authorizations for the products in this solution:  
  - “NGT Copy user authorizations” on page 93  
  - “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82  
  - “Setting LOADPLUS authorizations” on page 84  
  - “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120  
  - “Setting UNLOAD PLUS authorizations” on page 91  
  - “NGT Recover user authorizations” on page 97  
  - “NGT authorizations” on page 138  
  - “Configuring security for BMC Workbench” on page 101 |
| (optional) Enabling interaction between products | If you did not install this solution at the same time as the Administrative products, you might need to complete the following tasks:  
  - See “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153.  
  - See “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151. |
| Completing tasks specific to CATALOG MANAGER, ALTER, and CHANGE MANAGER | See Table 7 on page 20.                                                                 |
| Completing tasks specific only to CATALOG MANAGER | See Table 8 on page 22.                                                                |
The following tables list additional customization tasks that apply to specific products or components within the solution.

### Table 7: Specific CATALOG MANAGER, ALTER, and CHANGE MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(optional)</em> Defining catalog indirection</td>
<td>Catalog indirection is an optional method of implementing and maintaining CATALOG MANAGER, ALTER, and CHANGE MANAGER. See “Using catalog indirection with ALTER, CATALOG MANAGER, and CHANGE MANAGER” on page 182.</td>
</tr>
<tr>
<td>Working with CLISTs</td>
<td>Ensure that the correct version of CLIST is installed and that implicit execution of CLISTs is enabled. See “Working with CLISTs” on page 211.</td>
</tr>
<tr>
<td><em>(optional)</em> Creating indexes to improve performance</td>
<td>To improve performance, BMC recommends that you create indexes on the DB2 catalog tables and on copies of the catalog tables (if you are using catalog indirection). See “Creating indexes to improve performance” on page 163.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
| **Sharing components** | The ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products share several components. You must bind each product to the new level of the shared components if either of the following conditions exists:  
  - You install the products at different times  
  - You are applying maintenance, and some of the products share the same APF-authorized load library.  
  See “Shared components” on page 163. |
| *(optional) Customizing the BMCDB2PR panel* | The BMCDB2PR panel is part of the ISPF interface that the Installation System generates.  
  You might need to add additional products to the selection list or modify the catalog access field after you install and customize ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS.  
  See “BMCDB2PR panel” on page 167. |
| *(optional) Customizing the control table* | By modifying the control table, you can:  
  - Add a product  
  - Specify the location of libraries  
  - Enable access to data sharing members  
  - Specify different libraries for SSIDs  
  - Specify shared installation options  
  See “Control table” on page 170. |
| *(optional) Enabling fast path navigation* | Fast Path Navigation enables you to switch from one product to another without leaving the current product. The Installation System provides Fast Path Navigation for the ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products.  
| *(optional) Changing user profile values* | You can change the values in the installation options module or in the product options file (POF) for a specific product by using the product’s user options.  
  See “Modifying user profile values” on page 180. |
| *(optional) Enabling the use of DDF* | CATALOG MANAGER and CHANGE MANAGER can access remote DB2 subsystems by using the DB2 Distributed Data Facility (DDF).  
  **Note:** Perform this task only if you did not enable the use of DDF when you installed the products.  
  See “Enabling the use of DDF” on page 193. |
### Table 8: Specific CATALOG MANAGER tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(optional)</em> Accessing catalog information</td>
<td>For an overview of the CATALOG MANAGER access guidelines, see “Access to catalog information” on page 187.</td>
</tr>
<tr>
<td><em>(optional)</em> Prohibiting access to CATALOG MANAGER functions</td>
<td>Set options for editing data, controlling data display, and processing SQL on the Edit DB2 Table Options panel. See “Prohibiting access to CATALOG MANAGER functions” on page 187.</td>
</tr>
<tr>
<td><em>(optional)</em> Specifying an entry panel</td>
<td>You can optionally cause CATALOG MANAGER to display an entry panel other than the Primary Menu panel by adding an entry panel command to the BMCDB2 CLIST. See “Specifying an entry panel” on page 188.</td>
</tr>
<tr>
<td><em>(optional)</em> Specifying locking options for editing data</td>
<td>To set the editor locking options for all users, you must enable the locking options command. See “Specifying locking options for editing data” on page 190.</td>
</tr>
<tr>
<td><em>(optional)</em> Setting the session profile</td>
<td>The CATALOG MANAGER session profile enables you to customize specific product displays and operations for specific users or groups of users. See “Setting the session profile” on page 191.</td>
</tr>
<tr>
<td><em>(optional)</em> Editing the CONNECT command servers</td>
<td>You can edit and change the servers that are listed for the CONNECT command. See “Editing the CONNECT command servers” on page 192.</td>
</tr>
<tr>
<td><em>(optional)</em> Adding ACTEMAIN and ACTDCL to the ISPF command table</td>
<td>System security can use a TSO command-limiting function to restrict an individual user or an entire site. If command limiting is active, you must add ACTEMAIN and ACTDCL to the list of commands that are allowed for CATALOG MANAGER. See “Adding ACTEMAIN and ACTDCL to the ISPF command table” on page 193.</td>
</tr>
<tr>
<td><em>(optional)</em> Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER</td>
<td>Within CATALOG MANAGER, you can use commands to invoke the SQL Explorer for DB2 product. See “Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER” on page 161.</td>
</tr>
</tbody>
</table>

### Table 9: LOADPLUS specific customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing products that prevent x37 abends in LOADPLUS</td>
<td>Products that prevent x37 abends must be customized to ensure that they work properly with EXCP processing in LOADPLUS. See “Customizing products that prevent x37 abends in LOADPLUS” on page 148.</td>
</tr>
<tr>
<td>Increasing the size of DB2 active logs for LOADPLUS</td>
<td>See “Increasing the size of DB2 active logs for LOADPLUS” on page 148.</td>
</tr>
</tbody>
</table>
In addition to the customization tasks for multiple components, the following task applies to EXTENDED BUFFER MANAGER for DB2 and SNAPSHOT UPGRADE FEATURE for DB2.

**Table 10: XBM and SUF specific customization tasks**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing XBM subsystems</td>
<td>See “Customizing XBM subsystems” on page 279.</td>
</tr>
<tr>
<td>Customizing XBM components</td>
<td>See “Customizing XBM components” on page 289.</td>
</tr>
</tbody>
</table>

**Table 11: Cross-System Image Manager (XIM) specific customization tasks**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing Cross-System Image Manager (XIM)</td>
<td>The customization process constructs the XIM started task procedure and the XIM initiator procedure in the HLQJCL data set. Configuring XIM involves copying these procedures into the appropriate libraries. See “Customizing Cross-System Image Manager (XIM)” on page 202.</td>
</tr>
<tr>
<td>Restricting access to the worklist parallelism feature</td>
<td>By default, user access to execute portions of a worklist concurrently and to start XIM dynamically is not restricted. You can control access to these functions for a user or a group of users. See “Restricting access to the worklist parallelism feature” on page 140.</td>
</tr>
<tr>
<td>Executing XIM</td>
<td>This solution uses the XIM technology to manage units of work (UOWs). See “Execution of XIM” on page 203.</td>
</tr>
</tbody>
</table>

**Table 12: NGT Load and Unload specific customization tasks**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up data set access and security settings</td>
<td>See “NGT data set access and security settings” on page 136.</td>
</tr>
<tr>
<td>Set up NGT authorizations</td>
<td>See “NGT authorizations” on page 138.</td>
</tr>
<tr>
<td>Setting up checkpoints</td>
<td>See “Checkpoint data set considerations” on page 307.</td>
</tr>
<tr>
<td>Configuring block sizes</td>
<td>See “Block size considerations” on page 308.</td>
</tr>
<tr>
<td>Specifying the global utility parameters</td>
<td>See the BMC Next Generation Technology General User Guide.</td>
</tr>
<tr>
<td>Specifying product-specific utility parameters</td>
<td>See the Parameters chapter of the reference manual for each product.</td>
</tr>
<tr>
<td>Setting up the NGT Utility Manager</td>
<td>See the BMC Next Generation Technology Utility Manager for DB2 for z/OS Reference Manual.</td>
</tr>
</tbody>
</table>
### Starting the NGT Subsystem

See “Starting NGT Subsystem” on page 308.
For more information, see the *BMC Next Generation Technology Subsystem Reference Manual*.

#### Table 13: BMC Workbench specific customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading the customization overview</td>
<td>This section provides important background information about customizing BMC Workbench. See “Customization overview” on page 293.</td>
</tr>
<tr>
<td>Installing SYSPROC.ADMIN_COMMAND_DSN</td>
<td>If you have not installed SYSPROC.ADMIN_COMMAND_DSN, then perform this task. See “BMC Workbench for DB2 requirements” on page 294.</td>
</tr>
<tr>
<td>(optional) Editing the BMC Workbench option set</td>
<td>The installation process automatically creates a default option set named GUDOPT that is based on definitions that you supply during installation. If required, you can edit this option set. See “Editing the BMC Workbench option set” on page 298.</td>
</tr>
<tr>
<td>Customizing Common Explain</td>
<td>Customize Common Explain for use with BMC Workbench. See “Common Explain” on page 300.</td>
</tr>
</tbody>
</table>

#### Table 14: Customization tasks for verifying installation

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying the installation of the Administrative products</td>
<td>Perform this task to verify that ALTER, CATALOG MANAGER, or CHANGE MANAGER have been installed correctly. See “Verifying the Administrative products’ installation” on page 327.</td>
</tr>
<tr>
<td>Verifying Backup and Recovery product and Utility product installation</td>
<td>The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job. See “Verifying Backup and Recovery product and Utility product installation” on page 328.</td>
</tr>
</tbody>
</table>
BMC Performance for DB2 SQL customization tasks

After you install and configure the BMC Performance for DB2SQL solution, you might need to perform several additional customization tasks to complete and verify the installation. You perform these tasks outside the Installation System dialog panels.

This solution includes the following products or components:

- APPTUNE for DB2
- SQL Explorer for DB2
- BMC Workbench for DB2

Perform the following customization tasks:

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read the overview section</td>
<td>The overview section contains important information, read the section before commencing the customization. See “Overview” on page 227.</td>
</tr>
<tr>
<td>Controlling access to BMC Performance for DB2SQL</td>
<td>See Table 16 on page 26.</td>
</tr>
<tr>
<td>Performing post-installation tasks</td>
<td>See Table 17 on page 26.</td>
</tr>
<tr>
<td>Customizing the BMC Performance for DB2SQL products</td>
<td>See Table 18 on page 28.</td>
</tr>
<tr>
<td>Completing tasks specific to BMC Workbench for DB2</td>
<td>See Table 19 on page 28.</td>
</tr>
<tr>
<td>Verifying product installation</td>
<td>See Table 20 on page 29.</td>
</tr>
</tbody>
</table>

The following tables list additional customization tasks that apply to specific products or components within the solution.
Table 16: Controlling access to the System and SQL Performance products

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing the user IDs for the DBC component</td>
<td>The DBC is the host address space that the System and SQL Performance products use. For an overview, see “User IDs for the DBC component” on page 103. For more specific information about required authorizations for DBC, see the section about the required authorizations for user IDs in the BMC Infrastructure Components Administration Guide.</td>
</tr>
<tr>
<td>Setting security and permissions for user IDs for the System and SQL Performance products</td>
<td>Multiple user IDs are associated with installing, configuring, and using the product. See “Security and permissions for user IDs for the System and SQL Performance products” on page 105.</td>
</tr>
<tr>
<td>Customizing the plan name</td>
<td>The System and SQL Performance products provide one plan. APPTUNE, SQL Explorer, MainView for DB2 - Data Collector, SQL Performance, and System Performance use this plan. Pool Advisor does not use a plan. See “Plan name” on page 105.</td>
</tr>
<tr>
<td>Granting authorizations for MVS security</td>
<td>If you have an IBM MVS security system, you must grant the required authorizations, even if your security system does not control access to DB2. See “MVS security” on page 106.</td>
</tr>
<tr>
<td>Considerations when using DBC with CA-AF2, CA-Top Secret, or RACF security</td>
<td>If you use the IBM RACF or the CA Technologies CA-ACF2 or CA-Top Secret security product to control access to DB2, considerations apply. See “Managing security with CA-ACF2, CA-Top Secret, or RACF security” on page 109.</td>
</tr>
<tr>
<td>Establishing DB2 and product security</td>
<td>The product administrator is responsible for establishing default security options for all users and for maintaining individual user access options through the user profile. See “DB2 and product security” on page 111.</td>
</tr>
</tbody>
</table>

**Note**
Perform the following tasks in the order in which they are presented. These tasks must be performed *only* once, even if you are installing multiple products.

Table 17: Post Installation tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining a DOMPLEX</td>
<td>See “Defining a DOMPLEX” on page 229.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
| **Editing a DOMPLEX option set online** | Use this procedure to edit the DOMPLEX option set through the online interface.  
See “Editing the DOMPLEX option set online” on page 230. |
| **Verifying the product for data sharing members** | Define a DB2 subsystem in the DOMPLEX option set for every data sharing member in the data sharing groups.  
See “Verifying the product for data sharing members” on page 233. |
| **Customizing the CLISTs for SQL Explorer and CATALOG MANAGER** | You can launch the Common Explain component from CATALOG MANAGER, enabling you to access and analyze SQL from CATALOG MANAGER. You can also launch the SQLX edit macro of the SQL Explorer product from a TSO Edit session outside the product environment to Explain or execute a single SQL statement.  
See “Customizing the CLISTs for SQL Explorer and CATALOG MANAGER” on page 234. |
| **Creating indexes to improve performance** | To improve performance, BMC recommends that you create indexes on the DB2 catalog.  
See “Creating indexes to improve performance” on page 236. |
| **(optional) Generating Help text from DB2 trace record field descriptions** | The Help job generates Help text from DB2 trace record field descriptions, which are located in the DSNWMSG5 member of the DB2 SDNIVPD data set. Run this job if you want to be able to retrieve DB2 field descriptions from DSNWMSG5 while using the product.  
See “Generating Help text from DB2 trace record field descriptions” on page 237. |
| **Editing or reviewing the DBC JCL procedure** | To use the DBC component, you must configure the DBC started task.  
See “Editing or reviewing the DBC JCL procedure” on page 237. |
| **(optional) Adding or replacing the CLIST member for the ISPF interface** | Add or replace the CLIST for the ISPF interface.  
See “Adding or replacing the CLIST member for the ISPF interface” on page 240. |
| **Making products available from a menu** | You can make products available from the menu.  
See “Making products available from a menu” on page 243. |
| **(optional) Invoking SQL Explorer directly** | To invoke the SQL Explorer for DB2 product directly, use the PSSECLIST that was customized during installation.  
See “Invoking SQL Explorer directly” on page 244. |
| **(optional) Invoking BMC products without LIBDEFs** | Complete this procedure if you have your own ISPF environment and do not want to invoke DOMCLIST with the LIBDEF command.  
See “Invoking System and SQL Performance products without LIBDEFs” on page 244. |
| **Verifying or changing the global resource enqueues** | This task is required for shared-DASD environments that use a global resource manager like GRS or MIM.  
See “Verifying or changing the global resource enqueues” on page 246. |
Customization task | Description and link
---|---
(optional) Refreshing the MVS Linklist Lookaside | Refresh the LINKLST data set only if both of the following conditions are true:
- You are using the MVS Linklist Lookaside (LLA) feature.
- You have installed the product load modules into a LINKLST data set.
See “Refreshing the MVS Linklist Lookaside” on page 246.

Verifying the product authorization | All BMC Software products require product authorization before you can use them.
See “Verifying the product authorization” on page 246.

### Table 18: Customizing the BMC Performance for DB2 SQL products

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying or customizing the DOMPLEX option set</td>
<td>DOMPLEX option sets define one or more Data Collectors for monitoring DB2. The Data Collectors run as DOM agents with the DBC subsystem. Required for full and SSID installations. This task is not required if you are installing only SQL Explorer or OPERTUNE. See “Verifying or customizing the DOMPLEX option set” on page 247.</td>
</tr>
<tr>
<td>Verifying or changing the DOMPLEX parameters</td>
<td>The DOMPLEX parameters affect all users and procedures that use the same DOMPLEX option set. This task is required for a new product installation. It is optional for a migration installation. See “Verifying or changing DOMPLEX parameters” on page 262.</td>
</tr>
<tr>
<td>Checking the default user profile</td>
<td>User Profiles define the operating characteristics for a product session, including the authorizations granted to individual users. See “Checking the default User Profile” on page 266.</td>
</tr>
<tr>
<td>Additional information about archiving and the Next Generation Logger (NGL)</td>
<td>You can set up a procedure to automatically generate an archive of a log file, and set up a post-processing job that is automatically submitted each time an archive procedure finishes. See “Additional information about archiving and the NGL” on page 269.</td>
</tr>
</tbody>
</table>

You must perform the following tasks to customize BMC Workbench:

### Table 19: BMC Workbench specific customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading the customization overview</td>
<td>This section provides important background information about customizing BMC Workbench. See “Customization overview” on page 293.</td>
</tr>
</tbody>
</table>
### Customization task

<table>
<thead>
<tr>
<th>Description and link</th>
<th>Installing SYSPROC.ADMIN_COMMAND_DSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have not installed SYSPROC.ADMIN_COMMAND_DSN, then perform this task. See “BMC Workbench for DB2 requirements” on page 294.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description and link</th>
<th>(optional) Editing the BMC Workbench option set</th>
</tr>
</thead>
<tbody>
<tr>
<td>The installation process automatically creates a default option set named GUDOPT that is based on definitions that you supply during installation. If required, you can edit this option set. See “Editing the BMC Workbench option set” on page 298.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description and link</th>
<th>Customizing Common Explain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize Common Explain for use with BMC Workbench. See “Common Explain” on page 300.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 20: Customization tasks for verifying installation

<table>
<thead>
<tr>
<th>Description and link</th>
<th>Customization task</th>
</tr>
</thead>
<tbody>
<tr>
<td>The product procedure (PROC) must be invoked to initialize the DBC. See “Starting the DBC subsystem” on page 330.</td>
<td></td>
</tr>
<tr>
<td>Checking the system console log messages</td>
<td></td>
</tr>
<tr>
<td>Watch the system console log for the messages issued by the product procedure (PROC). See “Checking the system console log messages” on page 331.</td>
<td></td>
</tr>
<tr>
<td>If you previously terminated your session, perform this task. Otherwise, the product’s main menu is still displayed. See “Starting a product session” on page 335.</td>
<td></td>
</tr>
<tr>
<td>The product selects a DOMPLEX automatically if there is a DOMPLEX with a compatible Data Collector active when you begin your session. See “Selecting a DOMPLEX” on page 335.</td>
<td></td>
</tr>
<tr>
<td>The successful execution of an Explain command confirms that the Report Manager is communicating with the Data Collector, that the Data Collector is communicating with DB2, that the DAA vrD1 plan is working, and that installation is complete. See “Issuing a dynamic Explain command” on page 336.</td>
<td></td>
</tr>
<tr>
<td>The display of the Index Component reports confirms that the Index Component of SQL Performance has been installed correctly. See “Accessing the Index Component reports” on page 340.</td>
<td></td>
</tr>
</tbody>
</table>
### BMC Performance for DB2 Databases customization tasks

After you install and configure the BMC Performance for DB2 Databases solution, you must customize the solution to operate in your environment. After you complete these post-installation tasks, the solution is ready for use.

This solution includes the following products or components:

- DASD MANAGER PLUS for DB2
- REORG PLUS for DB2
- BMC Next Generation Technology Reorg for DB2 for z/OS
- SNAPSHOT UPGRADE FEATURE for DB2 (SUF), which is a component of EXTENDED BUFFER MANAGER for DB2 (XBM)
- BMC Next Generation Technology Stats for DB2 for z/OS
- BMC Next Generation Technology Utility Manager for DB2 for z/OS
- BMC Workbench for DB2

### Table 21: Summary of BMC Performance for DB2 Databases customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling access and setting user authorizations</td>
<td>Use the following information to set the required authorizations for the products in this solution:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- “DASD MANAGER PLUS authorizations” on page 98.</td>
</tr>
<tr>
<td></td>
<td>- “Setting REORG PLUS authorizations” on page 88.</td>
</tr>
<tr>
<td></td>
<td>- “NGT authorizations” on page 138</td>
</tr>
<tr>
<td></td>
<td>- “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120.</td>
</tr>
</tbody>
</table>
### Customization task | Description and link
--- | ---
Starting and stopping the UIM server | You must start the User Interface Middleware (UIM) server to enable the ISPF-Export utility for DASD MANAGER PLUS. BMC recommends that you start the UIM server automatically as part of the IPL process. See “Starting and stopping the UIM server” on page 309. For more information about the ISPF-Export utility, see “Customizing the ISPF-Export utility for DASD MANAGER PLUS” on page 195.
Setting the MEMLIMIT system parameter | See “Setting the MEMLIMIT system parameter” on page 143.
Completing tasks specific to XBM and SUF | After you finish installing the product, you must customize EXTENDED BUFFER MANAGER (XBM) and SNAPSHOT UPGRADE FEATURE (SUF) to operate in your environment. See “EXTENDED BUFFER MANAGER for DB2 (XBM) and SNAPSHOT UPGRADE FEATURE for DB2 (SUF) customization tasks” on page 78.
Completing tasks specific to DASD MANAGER PLUS | See Table 22 on page 32.
Completing tasks specific to NGT Reorg, NGT Stats, and NGT Utility Manager | See Table 23 on page 33
Completing tasks specific to BMC Workbench | See Table 24 on page 33.
Verifying installation of the REORG PLUS and DASD MANAGER PLUS components | See Table 25 on page 34.
*(optional)* Enabling interaction with other BMC Software products | If you did not install this solution at the same time as the Administrative products, you might need to complete the following tasks:
- “Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products)” on page 154
- “Enabling the use of DASD MANAGER PLUS within ALTER or CHANGE MANAGER” on page 156
- “Enabling the use of DASD MANAGER PLUS within CATALOG MANAGER” on page 158
- “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151
- “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153
*(optional)* Accessing multiple z/OS systems | See “Accessing multiple z/OS systems” on page 315.
The following tables list additional customization tasks that apply to specific products or components within the solution.

### Table 22: DASD MANAGER PLUS customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling REXX executables</td>
<td>See “Enabling REXX executables” on page 195.</td>
</tr>
<tr>
<td><em>(optional)</em> Creating indexes to improve performance</td>
<td>See “Creating indexes to improve performance” on page 163.</td>
</tr>
<tr>
<td>Working with CLISTS</td>
<td>See “Working with CLISTs” on page 211.</td>
</tr>
<tr>
<td><em>(optional)</em> Customizing the BMCDB2PR panel</td>
<td>The BMCDB2PR panel is part of the ISPF interface that the Installation System generates. You might need to add additional products to the selection list or modify the catalog access field after you install and customize ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS. See “BMCDB2PR panel” on page 167.</td>
</tr>
</tbody>
</table>
### Table 23: NGT utility specific customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up data set access and security settings</td>
<td>See “NGT data set access and security settings” on page 136.</td>
</tr>
<tr>
<td>Setting up NGT authorizations</td>
<td>See “NGT authorizations” on page 138.</td>
</tr>
<tr>
<td>Setting up checkpoints</td>
<td>See “Checkpoint data set considerations” on page 307.</td>
</tr>
<tr>
<td>Configuring block sizes</td>
<td>See “Block size considerations” on page 308.</td>
</tr>
<tr>
<td>Specifying the global utility parameters</td>
<td>See the <em>BMC Next Generation Technology General User Guide</em>.</td>
</tr>
<tr>
<td>Specifying product-specific parameters</td>
<td>See the &quot;Parameters&quot; chapter of the reference manual for each product</td>
</tr>
<tr>
<td>Setting up the NGT Utility Manager</td>
<td>See the <em>BMC Next Generation Technology Utility Manager for DB2 for z/OS Reference Manual</em>.</td>
</tr>
<tr>
<td>Starting the NGT Subsystem</td>
<td>See “Starting NGT Subsystem” on page 308.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the <em>BMC Next Generation Technology Subsystem Reference Manual</em>.</td>
</tr>
</tbody>
</table>

### Table 24: BMC Workbench specific customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading the customization overview</td>
<td>This section provides important background information about customizing BMC Workbench. See “Customization overview” on page 293.</td>
</tr>
<tr>
<td>Installing SYSPROC.ADMIN_COMMAND_DSN</td>
<td>If you have not installed SYSPROC.ADMIN_COMMAND_DSN, then perform this task.</td>
</tr>
<tr>
<td></td>
<td>See “BMC Workbench for DB2 requirements” on page 294.</td>
</tr>
<tr>
<td><em>(optional) Editing the BMC Workbench option set</em></td>
<td>The installation process automatically creates a default option set named GUDOPT that is based on definitions that you supply during installation. If required, you can edit this option set. See “Editing the BMC Workbench option set” on page 298.</td>
</tr>
<tr>
<td>Customizing Common Explain</td>
<td>Customize Common Explain for use with BMC Workbench.</td>
</tr>
<tr>
<td></td>
<td>See “Common Explain” on page 300.</td>
</tr>
</tbody>
</table>
## BMC Recovery for DB2 customization tasks

After you install and configure the BMC Recovery for DB2 solution, you must customize the components of BMC Recovery for DB2 to operate in your environment.

This solution includes the following products or components:

- APPLICATION RESTART CONTROL for DB2
- CHECK PLUS for DB2
- BMC Next Generation Technology Check for DB2 for z/OS
- BMC Next Generation Technology Copy for DB2 for z/OS
- Log Master for DB2
- BMC Next Generation Technology Recover for DB2 for z/OS
- RECOVERY MANAGER for DB2
- SNAPSHOT UPGRADE FEATURE for DB2 (SUF), which is a component of EXTENDED BUFFER MANAGER for DB2 (XBM)
- BMC Workbench for DB2

After you finish installing the solution, you must customize the components of BMC Recovery for DB2 to operate in your environment.

### Table 25: Customization tasks for verifying installation

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
</table>
| Verifying the installation of the Administrative products | Perform this task to verify that ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS have been installed correctly.  
See “Verifying the Administrative products’ installation” on page 327. |
| Verifying Backup and Recovery product and Utility product installation | The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job.  
See “Verifying Backup and Recovery product and Utility product installation” on page 328. |
### Table 26: Summary of BMC Recovery *for DB2* customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling access and setting user authorizations</td>
<td>Before you run the IVP jobs for the products that make up BMC Recovery <em>for DB2</em>, you must grant the appropriate user authorizations.</td>
</tr>
<tr>
<td></td>
<td>- “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82</td>
</tr>
<tr>
<td></td>
<td>- “RECOVERY MANAGER for DB2 user authorizations” on page 95</td>
</tr>
<tr>
<td></td>
<td>- For details, see the <em>APPLICATION RESTART CONTROL Customization Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>- “Setting CHECK PLUS authorizations” on page 82</td>
</tr>
<tr>
<td></td>
<td>- “NGT Copy user authorizations” on page 93</td>
</tr>
<tr>
<td></td>
<td>- “NGT Recover user authorizations” on page 97</td>
</tr>
<tr>
<td></td>
<td>- “Log Master for DB2 user authorizations” on page 114</td>
</tr>
<tr>
<td></td>
<td>- “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120</td>
</tr>
<tr>
<td></td>
<td>- “High-speed Apply Engine user authorizations” on page 128</td>
</tr>
<tr>
<td></td>
<td>- “NGT authorizations” on page 138</td>
</tr>
<tr>
<td></td>
<td>- DBC and LGC authorizations are required for PACLOG, see the section about the required authorizations for user IDs in the <em>BMC Infrastructure Components Administration Guide</em>.</td>
</tr>
<tr>
<td>Completing tasks specific to RECOVERY MANAGER</td>
<td>You must customize RECOVERY MANAGER to operate in your environment.</td>
</tr>
<tr>
<td></td>
<td>See Table 27 on page 37.</td>
</tr>
<tr>
<td>Completing tasks specific to XBM and SUF</td>
<td>After you finish installing the product, you must customize EXTENDED BUFFER MANAGER (XBM) and SNAPSHOT UPGRADE FEATURE (SUF) to operate in your environment.</td>
</tr>
<tr>
<td></td>
<td>See “EXTENDED BUFFER MANAGER for DB2 (XBM) and SNAPSHOT UPGRADE FEATURE for DB2 (SUF) customization tasks” on page 78.</td>
</tr>
</tbody>
</table>
### Customization task

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>(optional) Enabling interaction between products in the BMC Recovery for DB2 solution</td>
<td>If you did not install this solution at the same time as the Administrative products, you might need to complete the following tasks:</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between RECOVERY MANAGER and Log Master” on page 160</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between RECOVERY MANAGER and NGT Recover” on page 160</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between NGT Copy and RECOVERY MANAGER” on page 161</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between RECOVERY MANAGER and PACLOG” on page 161</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products)” on page 154</td>
</tr>
<tr>
<td>Customizing APPLICATION RESTART CONTROL for DB2</td>
<td>For details, see the APPLICATION RESTART CONTROL Customization Guide.</td>
</tr>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
<tr>
<td>Completing tasks specific to NGT Check</td>
<td>See Table 28 on page 37.</td>
</tr>
<tr>
<td>Completing tasks specific to BMC Workbench for DB2</td>
<td>See Table 29 on page 38.</td>
</tr>
<tr>
<td>Verifying Backup and Recovery product and Utility product installation</td>
<td>The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job. See “Verifying Backup and Recovery product and Utility product installation” on page 328.</td>
</tr>
</tbody>
</table>

The following tables list additional customization tasks that apply to specific products or components within the solution.
### Table 27: RECOVERY MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required temporary tables for RECOVERY MANAGER</td>
<td>RECOVERY MANAGER requires declared DB2 global temporary tables.</td>
</tr>
<tr>
<td></td>
<td>See “Required temporary tables for RECOVERY MANAGER” on page 221.</td>
</tr>
<tr>
<td>Preparing for archive logs greater than 64 KB tracks</td>
<td>To successfully use archive logs greater than 64 KB tracks, you must set up some SMS rules.</td>
</tr>
<tr>
<td></td>
<td>See “Preparing for archive logs greater than 64 KB tracks” on page 222.</td>
</tr>
<tr>
<td>Migrating from an earlier version of RECOVERY MANAGER</td>
<td>Additional tasks, which are dependent on the versions you are updating from and to, are necessary if you migrating from an earlier version of RECOVERY MANAGER.</td>
</tr>
<tr>
<td></td>
<td>See “Migrating from an earlier version of RECOVERY MANAGER” on page 361.</td>
</tr>
<tr>
<td>Setting up data sharing for RECOVERY MANAGER for DB2</td>
<td>Required if you have installed RECOVERY MANAGER for some of your DB2 subsystems and are now preparing to migrate to data sharing.</td>
</tr>
<tr>
<td></td>
<td>See “Setting up data sharing for RECOVERY MANAGER for DB2” on page 222.</td>
</tr>
<tr>
<td>RECOVERY MANAGER, LGC, and DBC</td>
<td>The DBC started task must be started in order to run RECOVERY.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER, LGC, and DBC” on page 223.</td>
</tr>
<tr>
<td>RECOVERY MANAGER for DB2 archive history file</td>
<td>You should create an archive history file for each DB2 subsystem on which disaster recovery procedures will be generated.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER for DB2 archive history file” on page 223.</td>
</tr>
<tr>
<td>RECOVERY MANAGER for DB2 option set</td>
<td>The ARM$OPTS, which is the default option set, contains information for all subsystems that share the RECOVERY MANAGER for DB2 load libraries and control files.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER for DB2 option set” on page 224.</td>
</tr>
<tr>
<td>RECOVERY MANAGER for DB2 packages</td>
<td>SYSPACKAGE in the DB2 catalog will need to be cleaned up by using the FREE command because each release of RECOVERY MANAGER introduces a new version of each package.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER for DB2 packages” on page 224.</td>
</tr>
<tr>
<td>RECOVERY MANAGER for DB2 repository</td>
<td>A repository is required for each DB2 subsystem. In a data sharing environment, one repository is required for each data sharing group.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER for DB2 repository” on page 224.</td>
</tr>
</tbody>
</table>

### Table 28: NGT utilities specific customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up data set access and security settings</td>
<td>See “NGT data set access and security settings” on page 136.</td>
</tr>
<tr>
<td>Setting up NGT authorizations</td>
<td>See “NGT authorizations” on page 138.</td>
</tr>
</tbody>
</table>
### NGT Database Administration for DB2 customization tasks

After you install and configure the BMC Next Generation Technology Database Administration for DB2 solution, you must customize the solution to operate in your environment. After you complete these post-installation tasks, the solution is ready for use.

This solution includes the following products or components:

- **CHANGE MANAGER for DB2**

---

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up checkpoints</td>
<td>See “Checkpoint data set considerations” on page 307.</td>
</tr>
<tr>
<td>Configuring block sizes</td>
<td>See “Block size considerations” on page 308.</td>
</tr>
<tr>
<td>Specifying the global utility parameters</td>
<td>See the <em>BMC Next Generation Technology General User Guide</em>.</td>
</tr>
<tr>
<td>Specifying NGT Check parameters</td>
<td>See the <em>BMC Next Generation Technology Check for DB2 for z/OS Reference Manual</em>.</td>
</tr>
<tr>
<td>Starting the NGT Subsystem</td>
<td>See “Starting NGT Subsystem” on page 308.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the <em>BMC Next Generation Technology Subsystem Reference Manual</em>.</td>
</tr>
</tbody>
</table>

### Table 29: BMC Workbench specific customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading the customization overview</td>
<td>This section provides important background information about customizing BMC Workbench. See “Customization overview” on page 293.</td>
</tr>
<tr>
<td>Installing SYSPROC.ADMIN_COMMAND_DSN</td>
<td>If you have not installed SYSPROC.ADMIN_COMMAND_DSN, then perform this task. See “BMC Workbench for DB2 requirements” on page 294.</td>
</tr>
<tr>
<td><em>(optional)</em> Editing the BMC Workbench option set</td>
<td>The installation process automatically creates a default option set named GUDOPT that is based on definitions that you supply during installation. If required, you can edit this option set. See “Editing the BMC Workbench option set” on page 298.</td>
</tr>
<tr>
<td>Customizing Common Explain</td>
<td>Customize Common Explain for use with BMC Workbench. See “Common Explain” on page 300.</td>
</tr>
</tbody>
</table>
- CATALOG MANAGER for DB2
- BMC Next Generation Technology Copy for DB2 for z/OS
- BMC Next Generation Technology Load for DB2 for z/OS
- SNAPSHOT UPGRADE FEATURE for DB2 (SUF), which is a component of EXTENDED BUFFER MANAGER for DB2 (XBM)
- BMC Next Generation Technology Unload for DB2 for z/OS

Perform the following customization tasks for the BMC Next Generation Technology Database Administration for DB2 solution, in the order listed.

Table 30: Summary of BMC Next Generation Technology Database Administration for DB2 customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying authorization</td>
<td>Verify that your BMC Authorization passwords are saved and copied to the correct library. See “Authorization verification” on page 81.</td>
</tr>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
</tbody>
</table>
| Controlling access and setting user authorizations | Use the following information to set the required authorizations for the products in this solution:  
  ■ “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82  
  ■ “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120  
  ■ “Restricting access to the worklist parallelism feature” on page 140  
  ■ “NGT authorizations” on page 138 |
| (optional) Enabling interaction between products    | If you did not install this solution at the same time as the Administrative products, you might need to complete the following tasks:  
  ■ See “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153  
  ■ See “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151 |
| Completing tasks specific to CATALOG MANAGER, ALTER, and CHANGE MANAGER | See Table 31 on page 40. |
The following tables list additional customization tasks that apply to specific products or components within the solution.

### Table 31: Specific CATALOG MANAGER, ALTER, and CHANGE MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(optional)</em> Defining catalog indirection</td>
<td>Catalog indirection is an optional method of implementing and maintaining CATALOG MANAGER, ALTER, and CHANGE MANAGER. See “Using catalog indirection with ALTER, CATALOG MANAGER, and CHANGE MANAGER” on page 182.</td>
</tr>
<tr>
<td>Working with CLISTs</td>
<td>Ensure that the correct version of CLIST is installed and that implicit execution of CLISTs is enabled. See “Working with CLISTs” on page 211.</td>
</tr>
<tr>
<td><em>(optional)</em> Creating indexes to improve performance</td>
<td>To improve performance, BMC recommends that you create indexes on the DB2 catalog tables and on copies of the catalog tables (if you are using catalog indirection). See “Creating indexes to improve performance” on page 163.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Sharing components                      | The ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products share several components. You must bind each product to the new level of the shared components if either of the following conditions exists:  
  ■ You install the products at different times  
  ■ You are applying maintenance, and some of the products share the same APF-authorized load library.  
  See “Shared components” on page 163.                                                                                                                                                                                                                                                                 |
| *(optional)* Customizing the BMCDB2PR panel | The BMCDB2PR panel is part of the ISPF interface that the Installation System generates.  
  You might need to add additional products to the selection list or modify the catalog access field after you install and customize ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS.  
  See “BMCDB2PR panel” on page 167.                                                                                                                                                                                                                                                                 |
| *(optional)* Customizing the control table | By modifying the control table, you can:  
  ■ Add a product  
  ■ Specify the location of libraries  
  ■ Enable access to data sharing members  
  ■ Specify different libraries for SSIDs  
  ■ Specify shared installation options  
  See “Control table” on page 170.                                                                                                                                                                                                                                                                 |
| *(optional)* Setting up fast path navigation | Fast Path Navigation enables you to switch from one product to another without leaving the current product. The Installation System provides Fast Path Navigation for the ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products.  
| *(optional)* Changing user profile values | You can change the values in the installation options module or in the product options file (POF) for a specific product by using the product’s user options.  
  See “Modifying user profile values” on page 180.                                                                                                                                                                                                                                                                 |
| *(optional)* Enabling the use of DDF     | CATALOG MANAGER and CHANGE MANAGER can access remote DB2 subsystems by using the DB2 Distributed Data Facility (DDF).  
  **Note:** Perform this task only if you did not enable the use of DDF when you installed the products.  
  See “Enabling the use of DDF” on page 193.                                                                                                                                                                                                                                                                 |
Table 32: Specific CATALOG MANAGER tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(optional) Accessing catalog information</strong></td>
<td>For an overview of the CATALOG MANAGER access guidelines, see “Access to catalog information” on page 187.</td>
</tr>
<tr>
<td><strong>(optional) Prohibiting access to CATALOG MANAGER functions</strong></td>
<td>Set options for editing data, controlling data display, and processing SQL on the Edit DB2 Table Options panel. See “Prohibiting access to CATALOG MANAGER functions” on page 187.</td>
</tr>
<tr>
<td><strong>(optional) Specifying an entry panel</strong></td>
<td>You can optionally cause CATALOG MANAGER to display an entry panel other than the Primary Menu panel by adding an entry panel command to the BMCDB2 CLIST. See “Specifying an entry panel” on page 188.</td>
</tr>
<tr>
<td><strong>(optional) Specifying locking options for editing data</strong></td>
<td>To set the editor locking options for all users, you must enable the locking options command. See “Specifying locking options for editing data” on page 190.</td>
</tr>
<tr>
<td><strong>(optional) Setting the session profile</strong></td>
<td>The CATALOG MANAGER session profile enables you to customize specific product displays and operations for specific users or groups of users. See “Setting the session profile” on page 191.</td>
</tr>
<tr>
<td><strong>(optional) Editing the CONNECT command servers</strong></td>
<td>You can edit and change the servers that are listed for the CONNECT command. See “Editing the CONNECT command servers” on page 192.</td>
</tr>
<tr>
<td><strong>(optional) Adding ACTEMAIN and ACTDCL to the ISPF command table</strong></td>
<td>System security can use a TSO command-limiting function to restrict an individual user or an entire site. If command limiting is active, you must add ACTEMAIN and ACTDCL to the list of commands that are allowed for CATALOG MANAGER. See “Adding ACTEMAIN and ACTDCL to the ISPF command table” on page 193.</td>
</tr>
<tr>
<td><strong>(optional) Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER</strong></td>
<td>Within CATALOG MANAGER, you can use commands to invoke the SQL Explorer for DB2 production. See “Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER” on page 161.</td>
</tr>
</tbody>
</table>

Table 33: NGT utilities specific tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up data set access and security settings</td>
<td>See “NGT data set access and security settings” on page 136.</td>
</tr>
<tr>
<td>Setting up NGT authorizations</td>
<td>See “NGT authorizations” on page 138.</td>
</tr>
<tr>
<td>Setting up checkpoints</td>
<td>See “Checkpoint data set considerations” on page 307.</td>
</tr>
<tr>
<td>Configuring block sizes</td>
<td>See “Block size considerations” on page 308.</td>
</tr>
</tbody>
</table>
### Customization task

<table>
<thead>
<tr>
<th>Specification</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying the global utility parameters</td>
<td>See the <em>BMC Next Generation Technology General User Guide</em>.</td>
</tr>
<tr>
<td>Specifying product-specific parameters</td>
<td>See the Parameters chapter of the reference manual for each product.</td>
</tr>
<tr>
<td>Starting the NGT Subsystem</td>
<td>See “Starting NGT Subsystem” on page 308. For more information, see the <em>BMC Next Generation Technology Subsystem Reference Manual</em>.</td>
</tr>
</tbody>
</table>

### Table 34: XBM and SUF specific tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing XBM subsystems</td>
<td>See “Customizing XBM subsystems” on page 279.</td>
</tr>
<tr>
<td>Customizing XBM components</td>
<td>See “Customizing XBM components” on page 289.</td>
</tr>
</tbody>
</table>

### Table 35: Cross-System Image Manager (XIM) specific tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing Cross-System Image Manager (XIM)</td>
<td>The customization process constructs the XIM started task procedure and the XIM initiator procedure in the HLQ.JCL data set. Customizing XIM involves copying these procedures into the appropriate libraries. See “Customizing Cross-System Image Manager (XIM)” on page 202.</td>
</tr>
<tr>
<td>Executing XIM</td>
<td>The Database Administration solution uses the XIM technology to manage units of work (UOWs). See “Execution of XIM” on page 203.</td>
</tr>
</tbody>
</table>

### Table 36: Customization tasks for verifying installation

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying the installation of the Administrative products</td>
<td>Perform this task to verify that ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS have been installed correctly. See “Verifying the Administrative products’ installation” on page 327.</td>
</tr>
<tr>
<td>Verifying Backup and Recovery product and Utility product installation</td>
<td>The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job. See “Verifying Backup and Recovery product and Utility product installation” on page 328.</td>
</tr>
</tbody>
</table>
NGT Database Performance for DB2 customization tasks

After you install and configure the BMC Next Generation Technology Database Performance for DB2 solution, you must customize the solution to operate in your environment. After you complete these post-installation tasks, the solution is ready for use.

This solution includes the following products or components:

- BMC Next Generation Technology Reorg for DB2 for z/OS
- BMC Next Generation Technology Stats for DB2 for z/OS
- BMC Next Generation Technology Utility Manager for DB2 for z/OS
- SNAPSHOT UPGRADE FEATURE for DB2 (SUF), which is a component of EXTENDED BUFFER MANAGER for DB2 (XBM)

Table 37: Summary of NGT Database Performance for DB2 customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
</table>
| Controlling access and setting user authorizations | Use the following information to set the required authorizations for the products in this solution:  
  
  ■ “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120  
  
  ■ “NGT authorizations” on page 138                                                                                                           |
| Starting and stopping the UIM server            | You must start the User Interface Middleware (UIM) server to enable the ISPF-Export utility for DASD MANAGER PLUS. BMC recommends that you start the UIM server automatically as part of the IPL process.  
  
  See “Starting and stopping the UIM server” on page 309.                                                                                       |
| Setting the MEMLIMIT system parameter          | See “Setting the MEMLIMIT system parameter” on page 143.                                                                                              |
| Completing tasks specific to XBM and SUF        | After you finish installing the product, you must customize EXTENDED BUFFER MANAGER (XBM) and SNAPSHOT UPGRADE FEATURE (SUF) to operate in your environment.  
  
  See “EXTENDED BUFFER MANAGER for DB2 (XBM) and SNAPSHOT UPGRADE FEATURE for DB2 (SUF) customization tasks” on page 78.                        |
| Completing tasks specific to NGT Reorg, NGT Stats, and NGT Utility Manager | See Table 38 on page 45.                                                                                                                                  |
The following tables list additional customization tasks that apply to specific products or components within the solution.

**Table 38: Customization tasks for NGT utilities**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up data set access and security settings</td>
<td>See “NGT data set access and security settings” on page 136.</td>
</tr>
<tr>
<td>Setting up NGT authorizations</td>
<td>See “NGT authorizations” on page 138.</td>
</tr>
<tr>
<td>Setting up checkpoints</td>
<td>See “Checkpoint data set considerations” on page 307.</td>
</tr>
<tr>
<td>Configuring block sizes</td>
<td>See “Block size considerations” on page 308.</td>
</tr>
<tr>
<td>Specifying the global utility parameters</td>
<td>See the <em>[BMC Next Generation Technology General User Guide]</em>.</td>
</tr>
<tr>
<td>Specifying product-specific parameters</td>
<td>See the &quot;Parameters&quot; chapter of the reference manual for each product.</td>
</tr>
<tr>
<td>Setting up the NGT Utility Manager</td>
<td>See the <em>[BMC Next Generation Technology Utility Manager for DB2 for z/OS Reference Manual]</em>.</td>
</tr>
<tr>
<td>Starting the NGT Subsystem</td>
<td>See “Starting NGT Subsystem” on page 308. For more information, see the <em>[BMC Next Generation Technology Subsystem Reference Manual]</em>.</td>
</tr>
</tbody>
</table>

**Table 39: Customization tasks for verifying installation**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying the installation of the Administrative products</td>
<td>Perform this task to verify that ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS have been installed correctly. See “Verifying the Administrative products’ installation” on page 327.</td>
</tr>
</tbody>
</table>
The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job.

See “Verifying Backup and Recovery product and Utility product installation” on page 328.

**BMC Administrative Assistant for DB2 customization tasks**

After you install and configure the BMC Administrative Assistant for DB2 solution, you might need to perform several additional customization tasks to complete and verify the installation. You perform these tasks outside the Installation System dialog panels.

This solution includes the following products or components:

- ALTER for DB2
- CATALOG MANAGER for DB2
- BMC Next Generation Technology Recover for DB2 for z/OS (partial functionality)
- UNLOAD PLUS for DB2 (partial functionality)

Complete the following tasks in the order that they are listed.

**Table 40: Summary of BMC Administrative Assistant for DB2 customization tasks**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
</table>
| Verifying authorization | Verify that your BMC Authorization passwords are saved and copied to the correct library.  
See “Authorization verification” on page 81. |
<p>| Setting the MEMLIMIT system parameter | See “Setting the MEMLIMIT system parameter” on page 143. |</p>
<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
</table>
| Controlling access and setting user authorizations | Use the following information to set the required authorizations for the products in this solution:  
  ■ “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82  
  ■ “NGT Recover user authorizations” on page 97  
  ■ “Setting UNLOAD PLUS authorizations” on page 91 |
| *(optional)* Enabling interaction between products | You must enable interaction between these products and the utilities, if you installed CATALOG MANAGER, ALTER, or CHANGE MANAGER in these circumstances:  
  ■ In a separate installation session before you installed the Utility products  
  ■ Either in the same installation session as the Utility products or in a separate installation session after you installed the Utility products, but you did not associate ALTER or CHANGE MANAGER with the Utility products on the Product to Product Interface panel |
| Completing tasks specific to CATALOG MANAGER and ALTER | These tasks customize the CATALOG MANAGER, ALTER and CHANGE MANAGER components of the solution. See Table 41 on page 48. |
| Completing tasks specific to CATALOG MANAGER only | These tasks customize the CATALOG MANAGER component of the solution. See Table 42 on page 49. |
| Verifying product installation | Verifies that the components have been correctly installed. See Table 43 on page 50. |

The following tables list additional customization tasks that apply to specific products or components within the solution.

*Note*

The tasks listed in Table 41 on page 48 need to be performed only once, and affect all of the products included in the Administrative Assistant solution.
Table 41: Specific CATALOG MANAGER and ALTER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(optional)</em> Defining catalog indirection</td>
<td>Catalog indirection is an optional method of implementing and maintaining CATALOG MANAGER, ALTER, and CHANGE MANAGER. See “Using catalog indirection with ALTER, CATALOG MANAGER, and CHANGE MANAGER” on page 182.</td>
</tr>
<tr>
<td>Working with CLISTs</td>
<td>Ensure that the correct version of CLIST is installed and that implicit execution of CLISTs is enabled. See “Working with CLISTs” on page 211.</td>
</tr>
<tr>
<td><em>(optional)</em> Creating indexes to improve performance</td>
<td>To improve performance, BMC recommends that you create indexes on the DB2 catalog tables and on copies of the catalog tables (if you are using catalog indirection). See “Creating indexes to improve performance” on page 163.</td>
</tr>
</tbody>
</table>
| Sharing components                                         | The ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products share several components. You must bind each product to the new level of the shared components if either of the following conditions exists:  
  - You install the products at different times  
  - You are applying maintenance, and some of the products share the same APF-authorized load library. See “Shared components” on page 163. |
| *(optional)* Customizing the BMCDB2PR panel                | The BMCDB2PR panel is part of the ISPF interface that the Installation System generates. You might need to add additional products to the selection list or modify the catalog access field after you install and customize ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS. See “BMCDB2PR panel” on page 167. |
| *(optional)* Customizing the control table                 | By modifying the control table, you can:  
  - Add a product  
  - Specify the location of libraries  
  - Enable access to data sharing members  
  - Specify different libraries for SSIDs  
  - Specify shared installation options See “Control table” on page 170. |
### Customization task | Description and link
--- | ---

*(optional)* Changing user profile values | You can change the values in the installation options module or in the product options file (POF) for a specific product by using the product’s user options. See “Modifying user profile values” on page 180.

*(optional)* Enabling the use of DDF | CATALOG MANAGER and CHANGE MANAGER can access remote DB2 subsystems by using the DB2 Distributed Data Facility (DDF). Note: Perform this task only if you did not enable the use of DDF when you installed the products. See “Enabling the use of DDF” on page 193.

### Table 42: Specific CATALOG MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(optional)</em> Accessing catalog information</td>
<td>For an overview of the CATALOG MANAGER access guidelines, see “Access to catalog information” on page 187.</td>
</tr>
<tr>
<td><em>(optional)</em> Prohibiting access to CATALOG MANAGER functions</td>
<td>Set options for editing data, controlling data display, and processing SQL on the Edit DB2 Table Options panel. See “Prohibiting access to CATALOG MANAGER functions” on page 187.</td>
</tr>
<tr>
<td><em>(optional)</em> Specifying an entry panel</td>
<td>You can customize CATALOG MANAGER to display an entry panel other than the Primary Menu panel by adding an entry panel command to the BMCDB2 CLIST. See “Specifying an entry panel” on page 188.</td>
</tr>
<tr>
<td><em>(optional)</em> Specifying locking options for editing data</td>
<td>To set the editor locking options for all users, you must enable the locking options command. See “Specifying locking options for editing data” on page 190.</td>
</tr>
<tr>
<td><em>(optional)</em> Setting the session profile</td>
<td>You can customize the CATALOG MANAGER session profile to customize specific product displays and operations for specific users or groups of users. See “Setting the session profile” on page 191.</td>
</tr>
<tr>
<td><em>(optional)</em> Editing the CONNECT command servers</td>
<td>You can edit and change the servers that are listed for the CONNECT command. See “Editing the CONNECT command servers” on page 192.</td>
</tr>
</tbody>
</table>
### BMC Database Administration for DB2 customization tasks

After you install and configure the BMC Database Administration for DB2 solution, you might need to perform several additional customization tasks to complete and verify the installation. You perform these tasks outside the Installation System dialog panels.

This solution includes the following products or components:

- CHANGE MANAGER for DB2
- CATALOG MANAGER for DB2
- BMC Next Generation Technology Copy for DB2 for z/OS
- LOADPLUS for DB2
Perform the following customization tasks for the BMC Database Administration for DB2 solution, in the order listed.

### Table 44: Summary of BMC Database Administration for DB2 customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying authorization</td>
<td>Verify that your BMC Authorization passwords are saved and copied to the correct library. See “Authorization verification” on page 81.</td>
</tr>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
</tbody>
</table>
| Controlling access and setting user authorizations | Use the following information to set the required authorizations for the products in this solution:  
  - “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82  
  - “NGT Copy user authorizations” on page 93  
  - “Setting LOADPLUS authorizations” on page 84  
  - “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120  
  - “Setting UNLOAD PLUS authorizations” on page 91  
  - “NGT Recover user authorizations” on page 97  
  - “Restricting access to the worklist parallelism feature” on page 140 |
| (optional) Enabling interaction between products | If you did not install this solution at the same time as the Administrative products, you might need to complete the following tasks:  
  - See “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153  
  - See “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151 |
The following tables list additional customization tasks that apply to specific products or components within the solution.

### Table 45: Specific CATALOG MANAGER, ALTER, and CHANGE MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>(optional) Defining catalog indirection</td>
<td>Catalog indirection is an optional method of implementing and maintaining CATALOG MANAGER, ALTER, and CHANGE MANAGER. See “Using catalog indirection with ALTER, CATALOG MANAGER, and CHANGE MANAGER” on page 182.</td>
</tr>
<tr>
<td>Working with CLISTs</td>
<td>Ensure that the correct version of CLIST is installed and that implicit execution of CLISTs is enabled. See “Working with CLISTs” on page 211.</td>
</tr>
<tr>
<td>(optional) Creating indexes to improve performance</td>
<td>To improve performance, BMC recommends that you create indexes on the DB2 catalog tables and on copies of the catalog tables (if you are using catalog indirection). See “Creating indexes to improve performance” on page 163.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Sharing components                       | The ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products share several components. You must bind each product to the new level of the shared components if either of the following conditions exists:  
  ■ You install the products at different times  
  ■ You are applying maintenance, and some of the products share the same APF-authorized load library.  
  See “Shared components” on page 163. |
| *(optional)* Customizing the BMCDB2PR panel | The BMCDB2PR panel is part of the ISPF interface that the Installation System generates.  
  You might need to add additional products to the selection list or modify the catalog access field after you install and customize ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS.  
  See “BMCDB2PR panel” on page 167. |
| *(optional)* Customizing the control table | By modifying the control table, you can:  
  ■ Add a product  
  ■ Specify the location of libraries  
  ■ Enable access to data sharing members  
  ■ Specify different libraries for SSIDs  
  ■ Specify shared installation options  
  See “Control table” on page 170. |
| *(optional)* Setting up fast path navigation | Fast Path Navigation enables you to switch from one product to another without leaving the current product. The Installation System provides Fast Path Navigation for the ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products.  
| *(optional)* Changing user profile values | You can change the values in the installation options module or in the product options file (POF) for a specific product by using the product’s user options.  
  See “Modifying user profile values” on page 180. |
| *(optional)* Enabling the use of DDF       | CATALOG MANAGER and CHANGE MANAGER can access remote DB2 subsystems by using the DB2 Distributed Data Facility (DDF).  
  **Note:** Perform this task only if you did not enable the use of DDF when you installed the products.  
  See “Enabling the use of DDF” on page 193. |
### Table 46: Specific CATALOG MANAGER tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(optional)</em> Accessing catalog information</td>
<td>For an overview of the CATALOG MANAGER access guidelines, see “Access to catalog information” on page 187.</td>
</tr>
<tr>
<td><em>(optional)</em> Prohibiting access to CATALOG MANAGER functions</td>
<td>Set options for editing data, controlling data display, and processing SQL on the Edit DB2 Table Options panel.</td>
</tr>
<tr>
<td></td>
<td>See “Prohibiting access to CATALOG MANAGER functions” on page 187.</td>
</tr>
<tr>
<td><em>(optional)</em> Specifying an entry panel</td>
<td>You can optionally cause CATALOG MANAGER to display an entry panel other than the Primary Menu panel by adding an entry panel command to the BMCDB2 CLIST.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying an entry panel” on page 188.</td>
</tr>
<tr>
<td><em>(optional)</em> Specifying locking options for editing data</td>
<td>To set the editor locking options for all users, you must enable the locking options command.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying locking options for editing data” on page 190.</td>
</tr>
<tr>
<td><em>(optional)</em> Setting the session profile</td>
<td>The CATALOG MANAGER session profile enables you to customize specific product displays and operations for specific users or groups of users.</td>
</tr>
<tr>
<td></td>
<td>See “Setting the session profile” on page 191.</td>
</tr>
<tr>
<td><em>(optional)</em> Editing the CONNECT command servers</td>
<td>You can edit and change the servers that are listed for the CONNECT command.</td>
</tr>
<tr>
<td></td>
<td>See “Editing the CONNECT command servers” on page 192.</td>
</tr>
<tr>
<td><em>(optional)</em> Adding ACTEMAIN and ACTDCL to the ISPF command table</td>
<td>System security can use a TSO command-limiting function to restrict an individual user or an entire site. If command limiting is active, you must add ACTEMAIN and ACTDCL to the list of commands that are allowed for CATALOG MANAGER.</td>
</tr>
<tr>
<td></td>
<td>See “Adding ACTEMAIN and ACTDCL to the ISPF command table” on page 193.</td>
</tr>
<tr>
<td><em>(optional)</em> Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER</td>
<td>Within CATALOG MANAGER, you can use commands to invoke the SQL Explorer for DB2 production.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER” on page 161.</td>
</tr>
</tbody>
</table>

### Table 47: LOADPLUS specific tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing products that prevent x37 abends in LOADPLUS</td>
<td>Products that prevent x37 abends must be customized to ensure that they work properly with EXCP processing in LOADPLUS.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing products that prevent x37 abends in LOADPLUS” on page 148.</td>
</tr>
<tr>
<td>Increasing the size of DB2 active logs for LOADPLUS</td>
<td>See “Increasing the size of DB2 active logs for LOADPLUS” on page 148.</td>
</tr>
</tbody>
</table>
Table 48: XBM and SUF specific tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing XBM subsystems</td>
<td>See “Customizing XBM subsystems” on page 279.</td>
</tr>
<tr>
<td>Customizing XBM components</td>
<td>See “Customizing XBM components” on page 289.</td>
</tr>
</tbody>
</table>

Table 49: Cross-System Image Manager (XIM) specific tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing Cross-System Image Manager (XIM)</td>
<td>The customization process constructs the XIM started task procedure and the XIM initiator procedure in the HLQJCL data set. Customizing XIM involves copying these procedures into the appropriate libraries. See “Customizing Cross-System Image Manager (XIM)” on page 202.</td>
</tr>
<tr>
<td>Executing XIM</td>
<td>The Database Administration solution uses the XIM technology to manage units of work (UOWs). See “Execution of XIM” on page 203.</td>
</tr>
</tbody>
</table>

Table 50: Customization tasks for verifying installation

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying the installation of the Administrative products</td>
<td>Perform this task to verify that ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS have been installed correctly. See “Verifying the Administrative products’ installation” on page 327.</td>
</tr>
<tr>
<td>Verifying Backup and Recovery product and Utility product installation</td>
<td>The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job. See “Verifying Backup and Recovery product and Utility product installation” on page 328.</td>
</tr>
</tbody>
</table>

Database Performance *for DB2* customization tasks

After you finish install and configure the Database Performance *for DB2* solution, you must customize the solution to operate in your environment. After you complete these post-installation tasks, the solution is ready for use.

This solution includes the following products or components:
- DASD MANAGER PLUS for DB2
- REORG PLUS for DB2
- SNAPSHOT UPGRADE FEATURE for DB2 (SUF), which is a component of EXTENDED BUFFER MANAGER for DB2 (XBM)

Table 51: Summary of Database Performance for DB2 customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling access and setting user authorizations</td>
<td>Use the following information to set the required authorizations for the products in this solution:</td>
</tr>
<tr>
<td></td>
<td>■ “DASD MANAGER PLUS authorizations” on page 98</td>
</tr>
<tr>
<td></td>
<td>■ “Setting REORG PLUS authorizations” on page 88</td>
</tr>
<tr>
<td></td>
<td>■ “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120</td>
</tr>
<tr>
<td>Starting and stopping the UIM server</td>
<td>You must start the User Interface Middleware (UIM) server to enable the ISPF-Export utility for DASD MANAGER PLUS. BMC recommends that you start the UIM server automatically as part of the IPL process. See “Starting and stopping the UIM server” on page 309. For more information about the ISPF-Export utility, see “Customizing the ISPF-Export utility for DASD MANAGER PLUS” on page 195.</td>
</tr>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
<tr>
<td>Completing tasks specific to XBM and SUF</td>
<td>After you finish installing the product, you must customize EXTENDED BUFFER MANAGER (XBM) and SNAPSHOT UPGRADE FEATURE (SUF) to operate in your environment. See “EXTENDED BUFFER MANAGER for DB2 (XBM) and SNAPSHOT UPGRADE FEATURE for DB2 (SUF) customization tasks” on page 78.</td>
</tr>
<tr>
<td>Completing tasks specific to DASD MANAGER PLUS</td>
<td>See Table 52 on page 58.</td>
</tr>
<tr>
<td>(optional) Verifying installation of the REORG PLUS and DASD MANAGER PLUS components</td>
<td>See Table 39 on page 45.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
| **(optional)** Enabling interaction with other BMC Software products | If you did not install this solution at the same time as the Administrative products, you might need to complete the following tasks:  
- “Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products)” on page 154  
- “Enabling the use of DASD MANAGER PLUS within ALTER or CHANGE MANAGER” on page 156  
- “Enabling the use of DASD MANAGER PLUS within CATALOG MANAGER” on page 158  
- “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151  
- “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153 |
| **(optional)** Accessing multiple z/OS systems | See “Accessing multiple z/OS systems” on page 315. |
| **(optional)** Merging multiple products into a single UIM server | See “Merging multiple products into a single UIM server” on page 323. |
| Sharing components | The ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products share several components. You must bind each product to the new level of the shared components if either of the following conditions exists:  
- You install the products at different times  
- You are applying maintenance, and some of the products share the same APF-authorized load library.  
See “Shared components” on page 163. |
| **(optional)** Changing installation options after customization | See “Modifying installation options after customization” on page 146. |
| **(optional)** Customizing the ISPF-Export utility for DASD MANAGER PLUS | See “Customizing the ISPF-Export utility for DASD MANAGER PLUS” on page 195. |

The following tables list additional customization tasks that apply to specific products or components within the solution.
Table 52: DASD MANAGER PLUS customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling REXX executables</td>
<td>See “Enabling REXX executables” on page 195.</td>
</tr>
<tr>
<td>Creating indexes to improve performance</td>
<td>See “Creating indexes to improve performance” on page 163.</td>
</tr>
<tr>
<td>Working with CLISTS</td>
<td>See “Working with CLISTs” on page 211.</td>
</tr>
<tr>
<td>(optional) Customizing the BMCDB2PR panel</td>
<td>The BMCDB2PR panel is part of the ISPF interface that the Installation System generates. You might need to add additional products to the selection list or modify the catalog access field after you install and customize ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS. See “BMCDB2PR panel” on page 167.</td>
</tr>
</tbody>
</table>

Table 53: Customization tasks for verifying installation

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying the installation of the Administrative products</td>
<td>Perform this task to verify that ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS have been installed correctly. See “Verifying the Administrative products’ installation” on page 327.</td>
</tr>
<tr>
<td>Verifying Backup and Recovery product and Utility product installation</td>
<td>The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job. See “Verifying Backup and Recovery product and Utility product installation” on page 328.</td>
</tr>
</tbody>
</table>

BMC Recovery Management for DB2 customization tasks

After you install and configure the BMC Recovery Management for DB2 solution, you must customize the components of BMC Recovery Management for DB2 to operate in your environment.
This solution includes the following products or components:

- BMC Next Generation Technology Copy for DB2 for z/OS
- Log Master for DB2
- R+/CHANGE ACCUM for DB2
- BMC Next Generation Technology Recover for DB2 for z/OS
- RECOVERY MANAGER for DB2
- SNAPSHOT UPGRADE FEATURE for DB2 (SUF), which is a component of EXTENDED BUFFER MANAGER for DB2 (XBM)

### Table 54: Summary of BMC Recovery Management for DB2 customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling access and setting user authorizations</td>
<td>Before you run the IVP jobs for the products that make up Recovery Management, you must grant the appropriate user authorizations.</td>
</tr>
<tr>
<td></td>
<td>- “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82</td>
</tr>
<tr>
<td></td>
<td>- “RECOVERY MANAGER for DB2 user authorizations” on page 95</td>
</tr>
<tr>
<td></td>
<td>- “NGT Copy user authorizations” on page 93</td>
</tr>
<tr>
<td></td>
<td>- “NGT Recover user authorizations” on page 97</td>
</tr>
<tr>
<td></td>
<td>- “Log Master for DB2 user authorizations” on page 114</td>
</tr>
<tr>
<td></td>
<td>- “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120</td>
</tr>
<tr>
<td></td>
<td>- “R+/CHANGE ACCUM for DB2 user authorizations” on page 118</td>
</tr>
<tr>
<td></td>
<td>- “High-speed Apply Engine user authorizations” on page 128</td>
</tr>
<tr>
<td></td>
<td>DBC and LGC authorizations are required for PACLOG, see the section about the required authorizations for user IDs in the BMC Infrastructure Components Administration Guide.</td>
</tr>
<tr>
<td>Completing tasks specific to RECOVERY MANAGER</td>
<td>You must customize RECOVERY MANAGER to operate in your environment.</td>
</tr>
<tr>
<td></td>
<td>See Table 55 on page 60.</td>
</tr>
<tr>
<td>Completing tasks specific to XBM and SUF</td>
<td>After you finish installing the product, you must customize EXTENDED BUFFER MANAGER (XBM) and SNAPSHOT UPGRADE FEATURE (SUF) to operate in your environment.</td>
</tr>
<tr>
<td></td>
<td>See “EXTENDED BUFFER MANAGER for DB2 (XBM) and SNAPSHOT UPGRADE FEATURE for DB2 (SUF) customization tasks” on page 78.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
| **(optional) Enabling interaction between products in the Recovery Management solution** | You might need to enable interaction between the following products:  
- “Enabling interaction between RECOVERY MANAGER and Log Master” on page 160  
- “Enabling interaction between RECOVERY MANAGER and NGT Recover” on page 160  
- “Enabling interaction between NGT Copy and RECOVERY MANAGER” on page 161  
- “Enabling interaction between RECOVERY MANAGER and PACLOG” on page 161  
- “Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products)” on page 154  
- “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153  
- “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151 |
| Setting the MEMLIMIT system parameter | See “Setting the MEMLIMIT system parameter” on page 143. |
| Verifying product installation | The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job.  
See “Verifying Backup and Recovery product and Utility product installation” on page 328. |

The following tables list additional customization tasks that apply to specific products or components within the solution.

Table 55: RECOVER MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
</table>
| Required temporary tables for RECOVERY MANAGER | RECOVERY MANAGER requires declared DB2 global temporary tables.  
See “Required temporary tables for RECOVERY MANAGER” on page 221. |
| Preparing for archive logs greater than 64 KB tracks | To successfully use archive logs greater than 64 KB tracks, you must set up some SMS rules.  
See “Preparing for archive logs greater than 64 KB tracks” on page 222. |
### Administrative products for DB2 customization tasks

If you have installed one or more Administrative products for DB2, but have not installed a solution that includes all of these products, you might need to perform several additional customization tasks to complete and verify the installation. You perform these tasks outside the Installation System dialog panels.

The Administrative products for DB2 include the following products:

- **ALTER for DB2**
- **CATALOG MANAGER for DB2**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrating from an earlier version of RECOVERY MANAGER</td>
<td>Additional tasks, which are dependent on the versions you are updating from and to, are necessary if you migrating from an earlier version of RECOVERY MANAGER. See “Migrating from an earlier version of RECOVERY MANAGER” on page 361.</td>
</tr>
<tr>
<td>Setting up data sharing for RECOVERY MANAGER for DB2</td>
<td>Required if you have installed RECOVERY MANAGER for some of your DB2 subsystems and are now preparing to migrate to data sharing. See “Setting up data sharing for RECOVERY MANAGER for DB2” on page 222.</td>
</tr>
<tr>
<td>RECOVERY MANAGER, LGC, and DBC</td>
<td>The DBC and LGC started tasks must be started in order to run RECOVERY. See “RECOVERY MANAGER, LGC, and DBC” on page 223.</td>
</tr>
<tr>
<td>RECOVERY MANAGER for DB2 archive history file</td>
<td>You should create an archive history file for each DB2 subsystem on which disaster recovery procedures will be generated. See “RECOVERY MANAGER for DB2 archive history file” on page 223.</td>
</tr>
<tr>
<td>RECOVERY MANAGER for DB2 option set</td>
<td>The ARM$OPTS, which is the default option set, contains information for all subsystems that share the RECOVERY MANAGER for DB2 load libraries and control files. See “RECOVERY MANAGER for DB2 option set” on page 224.</td>
</tr>
<tr>
<td>RECOVERY MANAGER for DB2 packages</td>
<td>SYSPACKAGE in the DB2 catalog will need to be cleaned up by using the FREE command because each release of RECOVERY MANAGER introduces a new version of each package. See “RECOVERY MANAGER for DB2 packages” on page 224.</td>
</tr>
<tr>
<td>RECOVERY MANAGER for DB2 repository</td>
<td>A repository is required for each DB2 subsystem. In a data sharing environment, one repository is required for each data sharing group. See “RECOVERY MANAGER for DB2 repository” on page 224.</td>
</tr>
</tbody>
</table>
Complete the following tasks in the order that they appear.

### Table 56: Customization tasks for all Administrative products

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying authorization</td>
<td>Verify that your BMC Authorization passwords are saved and copied to the correct library. See “Authorization verification” on page 81.</td>
</tr>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
<tr>
<td>(optional) Enabling interaction between products</td>
<td>You might need to enable interaction between the following products:</td>
</tr>
<tr>
<td></td>
<td>• See “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153</td>
</tr>
<tr>
<td></td>
<td>• See “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151</td>
</tr>
<tr>
<td></td>
<td>• See “Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products)” on page 154</td>
</tr>
</tbody>
</table>

Complete the following tasks that customize one or more products.

### Table 57: Customization tasks for multiple products

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>(optional) Defining catalog indirection</td>
<td>Catalog indirection is an optional method of implementing and maintaining CATALOG MANAGER, ALTER, and CHANGE MANAGER. See “Using catalog indirection with ALTER, CATALOG MANAGER, and CHANGE MANAGER” on page 182.</td>
</tr>
<tr>
<td>Working with CLISTs</td>
<td>Ensure that the correct version of CLIST is installed and that implicit execution of CLISTs is enabled. See “Working with CLISTs” on page 211.</td>
</tr>
<tr>
<td>(optional) Creating indexes to improve performance</td>
<td>To improve performance, BMC recommends that you create indexes on the DB2 catalog tables and on copies of the catalog tables (if you are using catalog indirection). See “Creating indexes to improve performance” on page 163.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Sharing components                     | The ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products share several components. You must bind each product to the new level of the shared components if either of the following conditions exists:  
  - You install the products at different times  
  - You are applying maintenance, and some of the products share the same APF-authorized load library.  
  See “Shared components” on page 163. |
| *(optional)* Customizing the BMCDB2PR panel | The BMCDB2PR panel is part of the ISPF interface that the Installation System generates. You might need to add additional products to the selection list or modify the catalog access field after you install and customize ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS.  
  See “BMCDB2PR panel” on page 167. |
| *(optional)* Customizing the control table | By modifying the control table, you can:  
  - Add a product  
  - Specify the location of libraries  
  - Enable access to data sharing members  
  - Specify different libraries for SSIDs  
  - Specify shared installation options  
  See “Control table” on page 170. |
| *(optional)* Enabling Fast Path Navigation | Fast Path Navigation enables you to switch from one product to another without leaving the current product. The Installation System provides Fast Path Navigation for the ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products.  
| *(optional)* Changing user profile values | You can change the values in the installation options module or in the product options file (POF) for a specific product by using the product’s user options.  
  See “Modifying user profile values” on page 180. |
| *(optional)* Enabling the use of DDF | CATALOG MANAGER and CHANGE MANAGER can access remote DB2 subsystems by using the DB2 Distributed Data Facility (DDF).  
  **Note:** Perform this task only if you did not enable the use of DDF when you installed the products.  
  See “Enabling the use of DDF” on page 193. |

In addition to the customization tasks for multiple components, you will need to perform customization tasks for CATALOG MANAGER.
### Table 58: Specific CATALOG MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>(optional) Accessing catalog information</td>
<td>For an overview of the CATALOG MANAGER access guidelines, see “Access to catalog information” on page 187.</td>
</tr>
<tr>
<td>(optional) Prohibiting access to CATALOG MANAGER functions</td>
<td>Set options for editing data, controlling data display, and processing SQL on the Edit DB2 Table Options panel. See “Prohibiting access to CATALOG MANAGER functions” on page 187.</td>
</tr>
<tr>
<td>(optional) Specifying an entry panel</td>
<td>You can optionally cause CATALOG MANAGER to display an entry panel other than the Primary Menu panel by adding an entry panel command to the BMCDB2 CLIST. See “Specifying an entry panel” on page 188.</td>
</tr>
<tr>
<td>(optional) Specifying locking options for editing data</td>
<td>To set the editor locking options for all users, you must enable the locking options command. See “Specifying locking options for editing data” on page 190.</td>
</tr>
<tr>
<td>(optional) Setting the session profile</td>
<td>The CATALOG MANAGER session profile enables you to customize specific product displays and operations for specific users or groups of users. See “Setting the session profile” on page 191.</td>
</tr>
<tr>
<td>(optional) Editing the CONNECT command servers</td>
<td>You can edit and change the servers that are listed for the CONNECT command. See “Editing the CONNECT command servers” on page 192.</td>
</tr>
<tr>
<td>(optional) Adding ACTEMAIN and ACTDCL to the ISPF command table</td>
<td>System security can use a TSO command-limiting function to restrict an individual user or an entire site. If command limiting is active, you must add ACTEMAIN and ACTDCL to the list of commands that are allowed for CATALOG MANAGER. See “Adding ACTEMAIN and ACTDCL to the ISPF command table” on page 193.</td>
</tr>
<tr>
<td>(optional) Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER</td>
<td>Within CATALOG MANAGER, you can use commands to invoke the SQL Explorer for DB2 product. See “Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER” on page 161.</td>
</tr>
</tbody>
</table>

In addition to the customization tasks for multiple products, you will need to perform tasks for DASD MANAGER PLUS.
Table 59: Specific DASD MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling DASD MANAGER PLUS use within other products</td>
<td>If you install DASD MANAGER PLUS after you have installed ALTER, CHANGE MANAGER, or CATALOG MANAGER, you must perform these additional procedures to use DASD MANAGER PLUS within these products. See “DASD MANAGER PLUS use within other products” on page 156.</td>
</tr>
<tr>
<td>Enabling REXX executables</td>
<td>The Installation System generates REXX executables for DASD MANAGER PLUS. These REXX executables can be implicitly executed. See “Enabling REXX executables” on page 195.</td>
</tr>
</tbody>
</table>

In addition to the customization tasks for multiple products, you must perform other tasks for NGT Recover and UNLOAD PLUS. These two products function as a technology component of some of the Administrative products.

Table 60: Specific NGT Recover and UNLOAD PLUS customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
<tr>
<td>Setting user authorizations for NGT Recover and UNLOAD PLUS</td>
<td>The NGT Recover product requires certain user authorizations. UNLOAD PLUS does not run as part of the DB2 subsystem. Therefore, users must have system authorizations and, for DIRECT YES, data set authorizations that are equivalent to the authorizations that DB2 requires. See “NGT Recover user authorizations” on page 97 and “Setting UNLOAD PLUS authorizations” on page 91.</td>
</tr>
</tbody>
</table>

After you configure and customize the products, you must verify the installation of the products.

Table 61: Customization tasks for verifying installation

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying the installation of the Administrative products</td>
<td>Perform this task to verify that ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS have been installed correctly. See “Verifying the Administrative products’ installation” on page 327.</td>
</tr>
</tbody>
</table>
Verifying product installation

The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job.

See “Verifying Backup and Recovery product and Utility product installation” on page 328.

## Backup and Recovery products for DB2 customization tasks

This section describes the customization tasks that you must complete for the Backup and Recovery products for DB2.

The Backup and Recovery products for DB2 include the following products:

- BMC Next Generation Technology Copy for DB2 for z/OS
- BMC Next Generation Technology Recover for DB2 for z/OS
- Log Master for DB2
- PACLOG for DB2
- R+/CHANGE ACCUM for DB2
- RECOVERY MANAGER for DB2

You must complete the customization tasks described in the following topics for the Backup and Recovery products for DB2.

### Table 62: Summary of generic customization tasks for Backup and Recovery products

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
</table>
| Controlling access and setting user authorizations | Before you run the IVP jobs for the products that you are installing, you should grant the appropriate DB2 and data set authorizations to your users.  
After you have granted the appropriate authorizations, complete any additional customization tasks for your installed products before verifying your installation.  
See Table 63 on page 67. |
| Completing tasks specific to RECOVERY MANAGER    | You must customize RECOVERY MANAGER to operate in your environment.                  
See Table 64 on page 68. |
### Customization task | Description and link
---|---
**Executing BCSS commands for PACLOG** | You must initialize the product in PACLOG processing only (PPO) mode. See “BCSS commands for PACLOG” on page 225.

**(optional) Enabling interaction between products** | You might need to enable interaction between the following products:

- “Enabling interaction between RECOVERY MANAGER and Log Master” on page 160
- “Enabling interaction between RECOVERY MANAGER and NGT Recover” on page 160
- “Enabling interaction between NGT Copy and RECOVERY MANAGER” on page 161
- “Enabling interaction between RECOVERY MANAGER and PACLOG” on page 161
- “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151
- “Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products)” on page 154
- “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153

**Setting the MEMLIMIT system parameter** | See “Setting the MEMLIMIT system parameter” on page 143.

**Verifying product installation** | The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job. See “Verifying Backup and Recovery product and Utility product installation” on page 328.

### Table 63: Required user authorizations

| Customization task | Description and link |
---|---|
**Specifying authorization verification mechanisms for the Backup and Recovery products and Utility products** | See “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82.
### Customization task

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying RECOVERY MANAGER for DB2 user authorizations</td>
<td>See “RECOVERY MANAGER for DB2 user authorizations” on page 95.</td>
</tr>
<tr>
<td>Specifying NGT Copy user authorizations</td>
<td>See “NGT Copy user authorizations” on page 93.</td>
</tr>
<tr>
<td>Specifying NGT Recover user authorizations</td>
<td>See “NGT Recover user authorizations” on page 97.</td>
</tr>
<tr>
<td>Specifying Log Master for DB2 user authorizations</td>
<td>See “Log Master for DB2 user authorizations” on page 114.</td>
</tr>
<tr>
<td>Specifying PACLOG for DB2 user authorizations</td>
<td>See “PACLOG for DB2 user authorizations” on page 116.</td>
</tr>
<tr>
<td>Specifying R+/CHANGE ACCUM for DB2 user authorizations</td>
<td>See “R+/CHANGE ACCUM for DB2 user authorizations” on page 118.</td>
</tr>
<tr>
<td>Specifying High-speed Apply Engine user authorizations</td>
<td>See “High-speed Apply Engine user authorizations” on page 128.</td>
</tr>
<tr>
<td>Specifying DBC authorizations</td>
<td>See the section about the required authorizations for user IDs in the <em>BMC Infrastructure Components Administration Guide</em>.</td>
</tr>
</tbody>
</table>

You must customize RECOVERY MANAGER to operate in your environment.

### Table 64: RECOVERY MANAGER customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required temporary tables for RECOVERY MANAGER</td>
<td>RECOVERY MANAGER requires declared DB2 global temporary tables. See “Required temporary tables for RECOVERY MANAGER” on page 221.</td>
</tr>
<tr>
<td>Preparing for archive logs greater than 64 KB tracks</td>
<td>To successfully use archive logs greater than 64 KB tracks, you must set up some SMS rules. See “Preparing for archive logs greater than 64 KB tracks” on page 222.</td>
</tr>
<tr>
<td>Migrating from an earlier version of RECOVERY MANAGER</td>
<td>Additional tasks, which are dependent on the versions you are updating from and to, are necessary if you migrating from an earlier version of RECOVERY MANAGER. See “Migrating from an earlier version of RECOVERY MANAGER” on page 361.</td>
</tr>
<tr>
<td>Setting up data sharing for RECOVERY MANAGER</td>
<td>This is required if you have installed RECOVERY MANAGER for some of your DB2 subsystems and are now preparing to migrate to data sharing. See “Setting up data sharing for RECOVERY MANAGER for DB2” on page 222.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RECOVERY MANAGER, LGC, and DBC</td>
<td>The DBC started task must be started in order to run RECOVERY MANAGER.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER, LGC, and DBC” on page 223.</td>
</tr>
<tr>
<td>RECOVERY MANAGER archive history file</td>
<td>You should create an archive history file for each DB2 subsystem on which disaster</td>
</tr>
<tr>
<td></td>
<td>recovery procedures will be generated.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER for DB2 archive history file” on page 223.</td>
</tr>
<tr>
<td>RECOVERY MANAGER option set</td>
<td>The ARM$OPTS, which is the default option set, contains information for all subsystems</td>
</tr>
<tr>
<td></td>
<td>that share the RECOVERY MANAGER load libraries and control files.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER for DB2 option set” on page 224.</td>
</tr>
<tr>
<td>RECOVERY MANAGER packages</td>
<td>SYSPACKAGE in the DB2 catalog will need to be cleaned up by using the FREE command</td>
</tr>
<tr>
<td></td>
<td>because each release of RECOVERY MANAGER introduces a new version of each package.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER for DB2 packages” on page 224.</td>
</tr>
<tr>
<td>RECOVERY MANAGER repository</td>
<td>A repository is required for each DB2 subsystem. In a data sharing environment, one</td>
</tr>
<tr>
<td></td>
<td>repository is required for each data sharing group.</td>
</tr>
<tr>
<td></td>
<td>See “RECOVERY MANAGER for DB2 repository” on page 224.</td>
</tr>
</tbody>
</table>

### Utility products for DB2 customization tasks

Perform the following tasks to prepare the Utility products for use. These tasks are performed after installation and configuration.

The Utility products for DB2 include the following products:

- **CHECK PLUS for DB2**
- **LOADPLUS for DB2**
- **REORG PLUS for DB2**
- **UNLOAD PLUS for DB2**
Table 65: Summary of utility product customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling access and setting user authorizations</td>
<td>Use the following information to set the required authorizations for the products in this solution:</td>
</tr>
<tr>
<td></td>
<td>■ “Authorization verification mechanisms for the Backup and Recovery products and Utility products” on page 82</td>
</tr>
<tr>
<td></td>
<td>■ “Setting CHECK PLUS authorizations” on page 82</td>
</tr>
<tr>
<td></td>
<td>■ “Setting LOADPLUS authorizations” on page 84</td>
</tr>
<tr>
<td></td>
<td>■ “Setting REORG PLUS authorizations” on page 88</td>
</tr>
<tr>
<td></td>
<td>■ “Setting UNLOAD PLUS authorizations” on page 91</td>
</tr>
<tr>
<td>Customizing products that prevent x37 abends in LOADPLUS</td>
<td>See “Customizing products that prevent x37 abends in LOADPLUS” on page 148.</td>
</tr>
<tr>
<td>Increasing the size of DB2 active logs for LOADPLUS</td>
<td>See “Increasing the size of DB2 active logs for LOADPLUS” on page 148.</td>
</tr>
<tr>
<td>Setting the MEMLIMIT system parameter</td>
<td>See “Setting the MEMLIMIT system parameter” on page 143.</td>
</tr>
<tr>
<td>(optional) Enabling interaction between products</td>
<td>If you did not install this solution at the same time as the Administrative products, you might need to complete the following tasks:</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)” on page 153</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)” on page 151</td>
</tr>
<tr>
<td></td>
<td>■ “Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products)” on page 154</td>
</tr>
</tbody>
</table>
NGT utility products customization tasks

Perform the following tasks to prepare the NGT utility products for use. These tasks are performed after installation and configuration.

The NGT utility products for DB2 include the following products:

- BMC Next Generation Technology Check for DB2 for z/OS
- BMC Next Generation Technology Load for DB2 for z/OS
- BMC Next Generation Technology LOBMaster for DB2 for z/OS
- BMC Next Generation Technology Reorg for DB2 for z/OS
- BMC Next Generation Technology Stats for DB2 for z/OS
- BMC Next Generation Technology Unload for DB2 for z/OS
- BMC Next Generation Technology Utility Manager for DB2 for z/OS

Table 66: Summary of NGT utility product customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up data set access and security settings</td>
<td>See “NGT data set access and security settings” on page 136.</td>
</tr>
<tr>
<td>Setting up NGT authorizations</td>
<td>See “NGT authorizations” on page 138.</td>
</tr>
<tr>
<td>Setting up checkpoints</td>
<td>See “Checkpoint data set considerations” on page 307.</td>
</tr>
<tr>
<td>Configuring block sizes</td>
<td>See “Block size considerations” on page 308.</td>
</tr>
<tr>
<td>Specifying the global utility parameters</td>
<td>See the BMC Next Generation Technology General User Guide.</td>
</tr>
<tr>
<td>Specifying product-specific parameters</td>
<td>See the Parameters chapter of the reference manual for each product.</td>
</tr>
<tr>
<td>Setting up the NGT Utility Manager</td>
<td>See the BMC Next Generation Technology Utility Manager for DB2 for z/OS</td>
</tr>
<tr>
<td>Starting the NGT Subsystem</td>
<td>See “Starting NGT Subsystem” on page 308.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the BMC Next Generation Technology Subsystem Reference Manual.</td>
</tr>
</tbody>
</table>

System and SQL Performance products for DB2 customization tasks

This section applies to all System and SQL Performance products.
The SQL Performance for DB2 solution includes the following products:

- APPTUNE for DB2
- SQL Explorer for DB2

The following products are included in the System Performance for DB2 solution:

- CATALOG MANAGER for DB2
- OPERTUNE for DB2
- Pool Advisor for DB2
- R+/CHANGE ACCUM for DB2

**Note**

Some procedures and tasks in this section do not apply to all of the System and SQL Performance products. All instructions that apply to APPTUNE and SQL Explorer also apply to SQL Performance for DB2. All instructions that apply to Pool Advisor also apply to BMC System Performance for DB2.

### Table 67: Summary of System and SQL Performance products for DB2 customization tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading the overview section</td>
<td>The overview section contains important information, read the section before commencing the customization. See “Overview” on page 227.</td>
</tr>
<tr>
<td>Controlling access to the System and SQL Performance products for DB2</td>
<td>See Table 68 on page 73.</td>
</tr>
<tr>
<td>Performing post-installation tasks</td>
<td>See Table 69 on page 74.</td>
</tr>
<tr>
<td>Customizing the System and SQL Performance products</td>
<td>See Table 70 on page 75.</td>
</tr>
<tr>
<td>Verifying product installation</td>
<td>See Table 71 on page 76.</td>
</tr>
<tr>
<td>Customizing OPERTUNE</td>
<td>See Table 72 on page 78.</td>
</tr>
</tbody>
</table>

These tasks outline the security mechanisms for controlling access to System and SQL Performance products and components and to DB2.
### Table 68: Controlling access to the System and SQL Performance products

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing the user IDs for the DBC component</td>
<td>The DBC is the host address space that the System and SQL Performance products use. For an overview, see “User IDs for the DBC component” on page 103. For more specific information about required authorizations for DBC, see the section about the required authorizations for user IDs in the <em>BMC Infrastructure Components Administration Guide</em>.</td>
</tr>
<tr>
<td>Setting security and permissions for user IDs for the System and SQL Performance products</td>
<td>Multiple user IDs are associated with installing, configuring, and using the product. See “Security and permissions for user IDs for the System and SQL Performance products” on page 105.</td>
</tr>
<tr>
<td>Customizing the plan name</td>
<td>The System and SQL Performance products provide one plan. APPTUNE, SQL Explorer, MainView for DB2 - Data Collector, SQL Performance, and System Performance use this plan. Pool Advisor does not use a plan. See “Plan name” on page 105.</td>
</tr>
<tr>
<td>Granting authorizations for MVS security</td>
<td>If you have an IBM MVS security system, you must grant the required authorizations, even if your security system does not control access to DB2. See “MVS security” on page 106.</td>
</tr>
<tr>
<td>Considerations when using DBC with CA-AF2, CA-Top Secret, or RACF security</td>
<td>If you use the IBM RACF or the CA Technologies CA-ACF2 or CA-Top Secret security product to control access to DB2, considerations apply. See “Managing security with CA-ACF2, CA-Top Secret, or RACF security” on page 109.</td>
</tr>
<tr>
<td>Establishing DB2 and product security</td>
<td>The product administrator is responsible for establishing default security options for all users and for maintaining individual user access options through the user profile. See “DB2 and product security” on page 110.</td>
</tr>
</tbody>
</table>

When you finish using the Installation System to generate and execute installation JCL, you must perform various post-installation tasks to complete the installation process.

These tasks are common to the System and SQL Performance products. Perform these tasks in the order in which they are presented. These tasks must be performed *only once*, even if you are installing multiple products.
Table 69: Post Installation tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
</table>
| Defining a DOMPLEX | *(All System and SQL Performance products except OPERTUNE and SQL Explorer)*  
See “Defining a DOMPLEX” on page 229. |
| Editing a DOMPLEX option set online | Use this procedure to edit the DOMPLEX option set through the online interface.  
See “Editing the DOMPLEX option set online” on page 230. |
| Verifying the product for data sharing members | *(APPTUNE, SQL Explorer, and SQL Performance)*  
Define a DB2 subsystem in the DOMPLEX option set for every data sharing member in the data sharing groups.  
See “Verifying the product for data sharing members” on page 233. |
| Customizing the CLISTs for SQL Explorer and CATALOG MANAGER | *(SQL Explorer and SQL Performance)*  
You can launch the Common Explain component from CATALOG MANAGER, enabling you to access and analyze SQL from CATALOG MANAGER. You can also launch the SQLX edit macro of the SQL Explorer product from a TSO Edit session outside the product environment to Explain or execute a single SQL statement.  
See “Customizing the CLISTs for SQL Explorer and CATALOG MANAGER” on page 234. |
| Creating indexes to improve performance | *(APPTUNE, SQL Explorer, MainView for DB2 – Data Collector, System Performance, and SQL Performance. It does not apply to Pool Advisor when it is run as a stand-alone product)*  
To improve performance, BMC recommends that you create indexes on the DB2 catalog.  
See “Creating indexes to improve performance” on page 236. |
| Generating Help text from DB2 trace record field descriptions | *(optional for APPTUNE, Pool Advisor, MainView for DB2 - Data Collector, System Performance, and SQL Performance. It does not apply to SQL Explorer when it is run as a stand-alone product.)*  
The Help job generates Help text from DB2 trace record field descriptions, which are located in the DSNWMSGS member of the DB2 SDSNIVPD data set. Run this job if you want to be able to retrieve DB2 field descriptions from DSNWMSGS while using the product.  
See “Generating Help text from DB2 trace record field descriptions” on page 237. |
| Editing or reviewing the DBC JCL procedure | *(The task does not apply to SQL Explorer or OPERTUNE)*  
To use the DBC component, you must configure the DBC started task.  
See “Editing or reviewing the DBC JCL procedure” on page 237. |
<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding or replacing the CLIST member for the ISPF interface</td>
<td>Add or replace the CLIST for the ISPF interface. See “Adding or replacing the CLIST member for the ISPF interface” on page 240.</td>
</tr>
<tr>
<td><em>(optional)</em> Making products available from a menu</td>
<td>You can make products available from the menu. See “Making products available from a menu” on page 243.</td>
</tr>
<tr>
<td><em>(optional)</em> Invoking SQL Explorer directly</td>
<td>To invoke the SQL Explorer for DB2 product directly, use the PSSCLIST that was customized during installation. See “Invoking SQL Explorer directly” on page 244.</td>
</tr>
<tr>
<td><em>(optional)</em> Invoking BMC products without LIBDEFs</td>
<td>Complete this procedure if you have your own ISPF environment and do not want to invoke DOMCLIST with the LIBDEF command. See “Invoking System and SQL Performance products without LIBDEFS” on page 244.</td>
</tr>
<tr>
<td>Verifying or changing the global resource enqueues</td>
<td>This task is required for shared-DASD environments that use a global resource manager like GRS or MIM. See “Verifying or changing the global resource enqueues” on page 246.</td>
</tr>
<tr>
<td><em>(optional)</em> Refreshing the MVS Linklist Lookaside</td>
<td>Refresh the LINKLST data set only if both of the following conditions are true: ■ You are using the MVS Linklist Lookaside (LLA) feature. ■ You have installed the product load modules into a LINKLST data set. See “Refreshing the MVS Linklist Lookaside” on page 246.</td>
</tr>
<tr>
<td>Verifying the product authorization</td>
<td>All BMC Software products require product authorization before you can use them. See “Verifying the product authorization” on page 246.</td>
</tr>
</tbody>
</table>

This section describes how to start the System and SQL Performance products that you have installed, create or review profiles, and check key values to make them consistent with the standards at your site.

**Table 70: Customizing the System and SQL Performance products**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying or customizing the DOMPLEX option set</td>
<td>DOMPLEX option sets define one or more Data Collectors for monitoring DB2. The Data Collectors run as DOM agents with the DBC subsystem. Required for full and SSID installations. This task is not required if you are installing only SQL Explorer or OPERTUNE. See “Verifying or customizing the DOMPLEX option set” on page 247.</td>
</tr>
</tbody>
</table>
The verification tasks you perform will depend on the products you are installing.

**Table 71: Customization tasks for verifying installation**

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying or changing the DOMPLEX parameters</td>
<td>The DOMPLEX parameters affect all users and procedures that use the same DOMPLEX option set. This task is required for a new product installation. It is optional for a migration installation. See “Verifying or changing DOMPLEX parameters” on page 262.</td>
</tr>
<tr>
<td>Checking the default user profile</td>
<td>User Profiles define the operating characteristics for a product session, including the authorizations granted to individual users. See “Checking the default User Profile” on page 266.</td>
</tr>
<tr>
<td>Additional information about archiving and the Next Generation Logger (NGL)</td>
<td>You can set up a procedure to automatically generate an archive of a log file, and set up a post-processing job that is automatically submitted each time an archive procedure finishes. See “Additional information about archiving and the NGL” on page 269.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting the DBC subsystem</td>
<td><em>(Required for all products except SQL Explorer and OPERTUNE)</em> The product procedure (PROC) must be invoked to initialize the DBC. See “Starting the DBC subsystem” on page 330.</td>
</tr>
<tr>
<td>Checking the system console log messages</td>
<td><em>(Required for all products except SQL Explorer and OPERTUNE)</em> Watch the system console log for the messages issued by the product procedure (PROC). See “Checking the system console log messages” on page 331.</td>
</tr>
<tr>
<td>Starting a product session</td>
<td><em>(Required for all products)</em> If you previously terminated your session, perform this task. Otherwise, the product’s main menu is still displayed. See “Starting a product session” on page 335.</td>
</tr>
<tr>
<td>Selecting a DOMPLEX</td>
<td><em>(Required for all products except SQL Explorer and OPERTUNE)</em> The product selects a DOMPLEX automatically if there is a DOMPLEX with a compatible Data Collector active when you begin your session. See “Selecting a DOMPLEX” on page 335.</td>
</tr>
<tr>
<td>Customization task</td>
<td>Description and link</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Issuing a dynamic Explain command</td>
<td><em>(Required for:)</em>&lt;br&gt;SQL Explorer&lt;br&gt;APPTUNE&lt;br&gt;MainView for DB2 - Data Collector&lt;br&gt;SQL Performance)*&lt;br&gt;The successful execution of an Explain command confirms that the Report Manager is communicating with the Data Collector, that the Data Collector is communicating with DB2, that the DAAvrD1 plan is working, and that installation is complete. See “Issuing a dynamic Explain command” on page 336.</td>
</tr>
<tr>
<td>Accessing the Index Component reports</td>
<td><em>(Required for SQL Performance)</em>&lt;br&gt;The display of the Index Component reports confirms that the Index Component of SQL Performance has been installed correctly. See “Accessing the Index Component reports” on page 340.</td>
</tr>
<tr>
<td>Verifying the SQL Explorer installation</td>
<td><em>(Required for:)</em>&lt;br&gt;SQL Explorer&lt;br&gt;SQL Performance)*&lt;br&gt;To verify that SQL Explorer has been installed correctly, you must test the following functions:&lt;br&gt;■ Call Attach facility (CAF)&lt;br&gt;■ Impact Analysis&lt;br&gt;■ Distributed Data facility (DDF)&lt;br&gt;See “Verifying the SQL Explorer installation” on page 342.</td>
</tr>
<tr>
<td>Starting a Pool Advisor or System Performance reporting session</td>
<td><em>(Required for:)</em>&lt;br&gt;Pool Advisor&lt;br&gt;System Performance)*&lt;br&gt;See “Starting a Pool Advisor or System Performance reporting session” on page 349.</td>
</tr>
</tbody>
</table>

After you use the OS/390 and z/OS Installer to generate and execute installation JCL, you must also perform customization tasks to complete the installation and configuration process for the OPERTUNE product.
### Table 72: Customizing OPERTUNE

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copying the OPERTUNE procedure to a PROCLIB</td>
<td>This required task copies the OPERTUNE started task procedure needed to a PROCLIB. See “Copying the OPERTUNE procedure to a PROCLIB” on page 271.</td>
</tr>
<tr>
<td>Invoking the OPERTUNE CLIST or the common BMCDISPN panel</td>
<td>This required task enables the OPERTUNE CLIST or common BMCDISPN panel. See “Invoking the OPERTUNE CLIST or the common BMCDISPN panel” on page 273.</td>
</tr>
<tr>
<td>Creating an OPERTUNE system profile</td>
<td>Before you can access an OPERTUNE system, you must create a system profile. This task is required for full installation. See “Creating an OPERTUNE system profile” on page 274.</td>
</tr>
<tr>
<td>Defining security for OPERTUNE</td>
<td>This task defines security for using OPERTUNE. The task is required for full installation and optional for maintenance installation. See “Defining security for OPERTUNE” on page 275.</td>
</tr>
<tr>
<td>Starting the OPERTUNE started task</td>
<td>This required task starts the OPERTUNE started task. A sample started task is in the output JCL data set member DDTPROC. See “Starting the OPERTUNE started task” on page 276.</td>
</tr>
<tr>
<td>Preparing ISPF for OPERTUNE diagnostics</td>
<td>This task enables OPERTUNE to obtain a dump for diagnostic purposes. See “Preparing ISPF for OPERTUNE diagnostics” on page 277.</td>
</tr>
<tr>
<td>Establishing OPERTUNE communications</td>
<td>Optionally, you can establish communications between two or more OPERTUNE systems. See “Establishing OPERTUNE communications” on page 278.</td>
</tr>
</tbody>
</table>

### EXTENDED BUFFER MANAGER for DB2 (XBM) and SNAPSHOT UPGRADE FEATURE for DB2 (SUF) customization tasks

After you finish installing the product, you must customize the EXTENDED BUFFER MANAGER for DB2 (XBM) and SNAPSHOT UPGRADE FEATURE for DB2 (SUF) products to operate in your environment. You perform these tasks outside the Installation System.

Table 73 on page 79 lists the tasks that you must perform to customize the XBM and SUF. Complete the tasks in the order that they are presented.
Because SUF is a subcomponent of XBM, the process for installing and customizing the products is the same. The features that are enabled are determined by password authorization.

Table 73: EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE tasks

<table>
<thead>
<tr>
<th>Customization task</th>
<th>Description and link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Granting user authorizations for XBM</td>
<td>See “Granting user authorizations for EXTENDED BUFFER MANAGER” on page 120.</td>
</tr>
<tr>
<td>Customizing XBM subsystems</td>
<td>See “Customizing XBM subsystems” on page 279.</td>
</tr>
<tr>
<td>Customizing XBM components</td>
<td>See “Customizing XBM components” on page 289.</td>
</tr>
</tbody>
</table>
Authorizations and security

This chapter describes the authorizations that are required for each product.

Authorization verification

You can enter your BMC Authorization passwords when you install the products.

If you are a licensed user and have already received and entered the permanent BMC Authorization passwords, ensure that the appropriate authorization modules are saved and copied to the new library after you install the products. The authorization modules are created when you add the password.

**Note**

In earlier product versions, the Installation System placed passwords directly into the *HLQ.LOAD* library. The Installation System now places passwords in the *HLQ.BMCPSWD* library and copies the passwords to the *HLQ.BMCLINK* library or to your APF-authorized library.

For more details, see the Installation System documentation.

Alternatively, you can use the BMC Product Authorization utility to apply passwords and to change your CPU configuration.

**Note**

You can choose not to input passwords during installation of the products. However, if you are installing the UNLOAD PLUS or LOADPLUS utility and you are migrating data from an earlier release using UNLOAD PLUS or LOADPLUS, you must input passwords for these products before you run the migration jobs.
User authorizations

This section describes the authorizations that are required for some of the components.

Authorization verification mechanisms for the Backup and Recovery products and Utility products

The products use one of the following mechanisms to verify authorization:

- If the DB2 DSNX@XAC authorization exit is available for your system, the product uses this exit to verify authorization for external access. The exit is available from the following sources:

  — IBM provides a sample exit with DB2 for the IBM Resource Access Control Facility (RACF) component.

  — CA Technologies provides the DSNX@XAC exit with the CA-ACF2 and CA-Top Secret products.

  BMC recommends this mechanism for implementing external security. The access control authorization exit must be available in the STEPLIB, JOBLIB, linklist, or in the SYS3.DSN exit.

- If the DSNX@XAC exit is not available, the product uses the standard DB2 method to check security.

Granting user authorizations for the Utility products

Before you run the IVP jobs for the products that you are installing, you should grant the appropriate DB2 and data set authorizations to your users. This topic describes the authorizations that are required for each Utility product.

After you have granted the appropriate authorizations, complete any additional customization tasks for your installed products before verifying your installation.

Setting CHECK PLUS authorizations

CHECK PLUS does not run as part of the DB2 subsystem. Therefore, users must have system and data set authorizations that are equivalent to the authorizations that DB2 requires. Use the following procedures to set the necessary authorizations.
To set DB2 authorizations

1 For all check jobs, set the following authorizations:
   ■ Sufficient DB2 authority to execute the CHECK PLUS plan and all packages that the CHECK PLUS plan uses
   ■ Authorization equivalent to the authorization that the comparable IBM DB2 CHECK utility requires

   **Note**
The CHECK TABLESPACE command requires only the authority to execute the CHECK PLUS plans and packages.

2 To enable the use of the FORCE option to cancel DB2 threads that might prevent a successful drain during a check job, also grant the following authorizations:
   ■ DISPLAY privileges
   ■ One of the following authorities:
     — SYSADM
     — SYSOPR
     — SYSCTRL

   **Note**
   These authorizations might be implicit in the authority that the users have.

To enable data set access using the DB2 RACF ID

1 Specify OPNDB2ID=YES in your installation options.
   This option tells CHECK PLUS to use the DB2 RACF ID for data set access.

To enable data set access when not using the DB2 RACF ID

1 Specify OPNDB2ID=NO in your installation options.
   This option tells CHECK PLUS not to use the DB2 RACF ID for data set access.

2 If using RACF or a similar system security package to protect underlying data sets and the Integrated Catalog Facility (ICF) catalog of a table or index space, set a minimum of the levels of authorization shown in the following table:
### Table 74: Minimum levels of authority that CHECK PLUS requires

<table>
<thead>
<tr>
<th>Table or index space definition</th>
<th>To access DB2 data sets</th>
<th>To access the ICF catalog</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCAT-defined</td>
<td>READ</td>
<td>READ</td>
</tr>
<tr>
<td>STOGROUP-defined</td>
<td>READ</td>
<td>READ</td>
</tr>
</tbody>
</table>

The following steps illustrate one method for granting these data set authorizations when your site uses a system security package other than RACF:

#### Example

1. Associate users with a security group.
2. Grant EXECUTE privileges on the CHECK PLUS product program (ACKUMAIN) to the security group.
3. Grant the data set authorizations to ACKUMAIN.

### Setting LOADPLUS authorizations

LOADPLUS does not run as part of the DB2 subsystem. Therefore, users must have system and data set authorizations that are equivalent to the authorizations that DB2 requires. Use the following procedures to set the necessary authorizations.

#### To set DB2 authorizations

1. For all load jobs, grant the following authorizations:
   - Sufficient DB2 authority to execute the LOADPLUS plan and all packages that the LOADPLUS plan uses
   - Authorization equivalent to the authorization that the IBM DB2 LOAD utility requires

2. To enable loading tables that contain identity columns, also complete the following authorization steps:

   **Note**

   These additional authorizations might be implicit in the authorization that the users have.

   a. Grant SELECT privileges on the following DB2 tables:
      - SYSIBM.SYSSEQUENCES
To enable use of the UPDATEMAXA YES option to update the MAXASSIGNEDVAL column of the SYSIBM.SYSSEQUENCES table, complete the following steps:

1. Determine which of the following authorization IDs should have ALTER privileges for the table that is being loaded:
   - User ID of the job owner
   - INSTALL SYSADM

2. Ensure that the value for the UPDMAXA_AUTHID installation option reflects this determination.

3. Grant ALTER privileges on the table that is being loaded for the appropriate authorization ID.

To enable loading a table whose table space or index spaces are defined with DEFINE NO, also grant INSERT privileges on that table.

**Note**

INSERT privileges might be implicit in the authority that the users have.

To enable the use of the FORCE option to cancel DB2 threads that might prevent a successful drain during a load job, also grant the following authorizations:

- DISPLAY privileges
- One of the following authorities:
  - SYSADM
  - SYSOPR
  - SYSCTRL

**Note**

These authorizations might be implicit in the authority that the users have.

To enable zIIP processing and LOADPLUS features that use snapshot processing, ensure that you have the appropriate authorizations for XBM or SUF.

For information about security levels and authorizations for XBM, see the EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE User Guide.

To enable running an SQLAPPLY load, also grant the following authorizations:
When running an SQLAPPLY load, LOADPLUS passes processing during the COMBINED phase to the High-speed Apply Engine component of the BMC Log Master for DB2 product. High-speed Apply requires the following DB2 authorizations. The APTGRANT member of the High-speed Apply HLQ.LLQSAMP installation data set (where HLQ is the high-level qualifier that is set during installation and LLQ is the low-level qualifier or prefix set during installation) contains sample authorization statements.

You can use secondary authorization IDs to limit access as necessary for your site.

- **(Normally granted during High-speed Apply installation) EXECUTE privileges:**
  - EXECUTE privilege for the plan that High-speed Apply uses to access its own restart table and the catalog
  - EXECUTE privilege for the High-speed Apply restart package

- **(Normally granted after High-speed Apply installation) additional privileges:**
  - INSERT privileges on the table that a user is loading
  - INSERT, UPDATE, SELECT, and DELETE privileges on the High-speed Apply restart table
  - CREATE privileges for the collections that High-speed Apply creates
  - Bind privileges with the add option (BINDADD) for the plans and packages that High-speed Apply creates during apply processing

The High-speed Apply Engine provides several ways to grant the CREATE and BINDADD privileges. Some techniques avoid granting bind privileges to the user ID that runs High-speed Apply. For more information, see the High-speed Apply Engine Reference Manual.

**Note**
The pre-bound plan option, described in the High-speed Apply Engine Reference Manual, is not compatible with LOADPLUS.

**To enable data set access using the DB2 RACF ID**

1. Specify OPNDB2ID=YES in your installation options.

   This option tells LOADPLUS to use the DB2 RACF ID for data set access.
To enable data set access when not using the DB2 RACF ID

1 Specify OPNDB2ID=NO in your installation options.

   This option tells LOADPLUS not to use the DB2 RACF ID for data set access.

2 If using RACF or a similar system security package to protect underlying data sets and the Integrated Catalog Facility (ICF) catalog of a table or index space, set a minimum of the levels of authorization shown in the following table for all load jobs.

<table>
<thead>
<tr>
<th>Table 75: Minimum levels of authorization that LOADPLUS requires</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table or index space definition</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>VCAT-defined</td>
</tr>
<tr>
<td>STOGROUP-defined</td>
</tr>
</tbody>
</table>

The following steps illustrate one method for granting these data set authorizations when your site uses a system security package other than RACF:

1 Associate users with a security group.

2 Grant EXECUTE privileges on the LOADPLUS product program (AMUUMAIN) to the security group.

3 Grant the data set authorizations to AMUUMAIN.

4 To enable checking referential constraints during the load, also grant READ privileges on the primary index of the parent table for the table being loaded.

4 To enable using rename or FASTSWITCH processing, if you establish authority at a node lower than the highest node, grant the same privileges as shown in Table 75 on page 87 for the following data sets:

- When FASTSWITCH NO is in effect:
  - VCAT.BMCDBD.database.object.I0001
  - VCAT.BMCDBC.database.object.I0001
  - VCAT.OLDDBD.database.object.I0001
  - VCAT.OLDDBC.database.object.I0001
  - VCAT.BMCDBD.database.object.J0001
  - VCAT.BMCDBC.database.object.J0001
  - VCAT.OLDDBD.database.object.J0001
  - VCAT.OLDDBC.database.object.J0001
When FASTSWITCH YES is in effect:
— VCAT.BMCDBD.database.object.I0001
— VCAT.BMCDBC.database.object.I0001
— VCAT.BMCDBD.database.object.J0001
— VCAT.BMCDBC.database.object.J0001

Setting REORG PLUS authorizations

REORG PLUS does not run as part of the DB2 subsystem. Therefore, users must have system and data set authorizations that are equivalent to the authorizations that DB2 requires. Use the following procedures to set the necessary authorizations.

To set DB2 authorizations

1. For all reorganization jobs, grant the following authorizations:
   - Sufficient DB2 authority to execute the REORG PLUS plan and all packages that the REORG PLUS plan uses
   - Authorization equivalent to the authorization that the comparable IBM DB2 REORG utility requires

   **Note**
   REORG PLUS does not check for the DELETE privilege when the SELECT/DELETE option is used. REORG PLUS does not check for the UPDATE privilege when the UPDATE option is used.

2. To enable running a SHRLEVEL CHANGE reorganization, also grant the following additional authorities:
   - TRACE authority
   - MONITOR2 authority
   - DISPLAY authority (if not already granted to PUBLIC)

   **Note**
   These privileges might be implicit in the authority that the users have.

3. To enable reorganizing base table spaces that contain XML columns, also grant SELECT privileges on the following DB2 tables:
   - SYSIBM.SYSSEQUENCES
   - SYSIBM.SYSSEQUENCESDEP
Note

These privileges might be implicit in the authority that the users have.

4 To enable reorganizing user-defined XML indexes, also grant SELECT privileges on the SYSIBM.SYSXMLRELS DB2 table.

Note

These privileges might be implicit in the authority that the users have.

5 To enable using the DSRSEXIT user exit to update the DB2 catalog (in other words, the DSRSEXIT user exit has a default of YES for the BMC_ALTER_DB2_CATALOG variable), also complete the following steps:

   a For the ALTER TABLESPACE statement, grant one of the following privileges if the user is not the owner of the table space:
      ■ DBADM authority for the database that contains the table
      ■ SYSADM or SYSCTRL authority
      ■ System DBADM

   b For the ALTER INDEX or ALTER TABLE statement, grant one of the following privileges if the user is not the owner of the index:
      ■ Ownership of the table on which the index is defined
      ■ DBADM authority for the database that contains the table
      ■ SYSADM or SYSCTRL authority
      ■ System DBADM

6 To enable using the MAPTEXIT user exit, also grant the authority to create and drop objects on the DSNDB04 database.

7 To enable the use of the FORCE option to cancel DB2 threads that might prevent a successful drain during a reorganization job, also grant the following authorizations:

   ■ DISPLAY privileges

   ■ One of the following authorities:
      —SYSADM
      —SYSOPR
      —SYSCTRL
Note
These authorizations might be implicit in the authority that the users have.

8 To enable use of the EXTENDED BUFFER MANAGER (XBM) product or SNAPSHOT UPGRADE FEATURE (SUF) component of XBM, ensure that you have the appropriate authorizations for XBM or SUF.

For information about security levels and authorizations for XBM, see the EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE User Guide.

To enable data set access using the DB2 RACF ID

1 Specify OPNDB2ID=YES in your installation options.

This option tells REORG PLUS to use the DB2 RACF ID for data set access.

Note
Using OPNDB2ID=NO can improve performance, depending on the size of your data set profiles and the number of VSAM data sets that are involved in the reorganization.

To enable data set access when not using the DB2 RACF ID

1 Specify OPNDB2ID=NO in your installation options.

This option tells REORG PLUS not to use the DB2 RACF ID for data set access.

2 If using RACF or a similar system security package to protect underlying data sets and the Integrated Catalog Facility (ICF) catalog of a table or index space, grant a minimum of the following levels of authorization:
   - ALTER or CONTROL to access, update, and define DB2 data sets
   - UPDATE or CONTROL to access and update the ICF catalog
Example

The following steps illustrate one method for granting these data set authorizations when your site uses a system security package other than RACF:

1. Associate users with a security group.

2. Grant EXECUTE privileges on the REORG PLUS product program (ARUUMAIN) to the security group.

3. Grant the data set authorizations to ARUUMAIN.

3 To enable using rename or FASTSWITCH processing, if you establish authority at a node lower than the highest node, grant the same privileges as described in Step 2 on page 87 for the following data sets:
   - For STAGEDSN=BMC:
     - VCAT.BMCDBD.database.object.I0001
     - VCAT.BMCDBC.database.object.I0001
     - VCAT.OLDDBD.database.object.I0001
     - VCAT.OLDDBC.database.object.I0001
     - VCAT.BMCDBD.database.object.J0001
     - VCAT.BMCDBC.database.object.J0001
     - VCAT.OLDDDBD.database.object.J0001
     - VCAT.OLDDBC.database.object.J0001
   - For STAGEDSN=DSN (the default when you use the FASTSWITCH process):
     - VCAT.BMCDBD.database.object.I0001
     - VCAT.BMCDBC.database.object.I0001
     - VCAT.BMCDBD.database.object.J0001
     - VCAT.BMCDBC.database.object.J0001
     - VCAT.DSNDBD.database.object.S0001
     - VCAT.DSNDBC.database.object.S0001

Setting UNLOAD PLUS authorizations

UNLOAD PLUS does not run as part of the DB2 subsystem. Therefore, users must have system authorizations and, for DIRECT YES, data set authorizations that are equivalent to the authorizations that DB2 requires. Use the following procedures to set the necessary authorizations.

Note

If you are using UNLOAD PLUS with ALTER for DB2 or CHANGE MANAGER for DB2, UNLOAD PLUS functions in DIRECT YES mode only.
To set DB2 authorizations

1 For all load jobs, set the following authorizations:
   - Sufficient DB2 authority to execute the UNLOAD PLUS plan and all packages that the UNLOAD PLUS plan uses
   - Authorization equivalent to the authorization that the IBM DB2 UNLOAD utility requires

   **Note**
   UNLOAD PLUS enforces row- and column-level security only when DIRECT NO is in effect.

2 To enable the use of the FORCE option to cancel DB2 threads that might prevent a successful drain during an unload job, grant the following authorizations:
   - DISPLAY privileges
   - One of the following authorities:
     — SYSADM
     — SYSOPR
     — SYSCTRL

   **Note**
   These authorizations might be implicit in the authority that the users have.

3 To enable zIIP processing and SHRLEVEL CHANGE CONSISTENT YES, ensure that you have the appropriate authorizations for XBM or SUF.

   For information about security levels and authorizations for XBM, see the *EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE User Guide*.

To enable data set access using the DB2 RACF ID

1 Specify OPNDB2ID=YES in your installation options.

   This option tells UNLOAD PLUS to use the DB2 RACF ID for data set access.

To enable data set access when not using the DB2 RACF ID

When using DIRECT NO, UNLOAD PLUS uses DB2 to access data sets. In this case, users do not need the authorization described in this procedure.
1 Specify OPNDB2ID=NO in your installation options.

This option tells UNLOAD PLUS not to use the DB2 RACF ID for data set access.

2 If using RACF or a similar system security package to protect underlying data sets and the Integrated Catalog Facility (ICF) catalog of a table or index space, grant READ privileges for the following sources:
   - DB2 VSAM data sets
   - DB2 image copy data sets
   - DSN1COPY data sets
   - Inline copy data sets
   - Instant Snapshot copy data sets
   - Online consistent copy data sets
   - Cabinet copy data sets
   - VSAM FlashCopy data sets
   - VSAM linear data sets
   - Encrypted copy data sets that are created by NGT Copy
   - Key data sets for encrypted copies

The following steps illustrate one method for granting these data set authorizations when your site uses a system security package other than RACF:

1 Associate users with a security group.

2 Grant EXECUTE privileges on the UNLOAD PLUS product program (ADUUMAIN) to the security group.

3 Grant the data set authorizations to ADUUMAIN.

**NGT Copy user authorizations**

The BMC Next Generation Technology Copy for DB2 for z/OS product requires certain user authorizations.

**DB2 authorizations for BMC Next Generation Technology Copy for DB2 for z/OS**

To use the NGT Copy product, you must have the following DB2 authorizations:

- To run NGT Copy, you must have EXECUTE authority on the NGT Copy plan, and the plan owner must have EXECUTE authority to collection-id.* for the collections referenced by the plan.
For NGT Copy to process database objects, your primary or secondary authorization IDs must have one of the following authorities:

- Installation SYSADM, SYSADM, or SYSCTRL authority
- DBADM, DBCTRL, or DBMAINT authority for the database containing the named space
- IMAGCOPY, DISPLAYDB, STARTDB, and STOPDB authority for the database containing the named space
- DISPLAY (system wide) and IMAGCOPY, STARTDB, and STOPDB authority for the database that contains the named space

To copy the database (DSNDB01), you must have installation SYSADM, SYSADM, or SYSCTRL authority.

If you make SHRLEVEL CONCURRENT copies and set the installation option READONLY to LOCKTBL, you must also have SELECT authority for the tables that you are copying or be the owner of those tables.

To use the COPY ... RUNSTATS option, you must have the STATSAUTH privilege on the database.

Note
NGT Copy checks authorization by using the DB2 security exit if this exit is in place. For NGT Copy to correctly determine the status of the DB2 security exit, the library containing module DSNX@XAC (most commonly DSNEXIT) must be included in the NGT Copy STEPLIB.

APF authorizations for BMC Next Generation Technology Copy for DB2 for z/OS

NGT Copy uses system services that require APF authorization.

NGT Copy must reside in an APF-authorized library. All load modules loaded by NGT Copy must be authorized and must reside in APF-authorized libraries.

RACF authorizations for BMC Next Generation Technology Copy for DB2 for z/OS

Because NGT Copy does not run as part of the DB2 subsystem, you must have authorization equivalent to that required by DB2 to use NGT Copy.

When the NGT Copy installation option OPNDB2ID is set to NO, and when the underlying data set of a table space is protected by Resource Access Control Facility (RACF) or a similar security system, you must have sufficient authority to access and
modify the data set. For index spaces, you must have read access to the index data sets.

When the NGT Copy installation option OPNDB2ID is set to YES, the DB2 RACF ID is used to allow DB2 data sets to be opened.

**Note**
For security systems other than RACF, the installation option OPNDB2ID must be set to NO.

If your DB2 is specified in the RACF started procedures table (ICHRIN03) as a privileged or trusted task and no user ID is associated with the DB2 address space, you cannot use OPNDB2ID to allow NGT Copy to access the DB2 data sets. In this case, the user running NGT Copy must have RACF authority to access the data sets needed for copying.

**Note**
If you are using SHRLEVEL CHANGE with data sharing, NGT Copy reads the bootstrap data set (BSDS). Therefore, you need READ authorization for the BSDS. NGT Copy reads the group buffer pool checkpoint records from the BSDSs for the group if it detects that the space being copied is group buffer pool dependent.

**RECOVERY MANAGER for DB2 user authorizations**

The RECOVERY MANAGER for DB2 product requires certain user authorizations.

**RACF authorization for RECOVERY MANAGER**

The RACF security administrator must define an Open Multiple Virtual Storage (OMVS) segment for each RECOVERY MANAGER user.

The user ID assigned to the DBC started task must also have an OMVS segment defined.

The OMVS segment is required because DBC utilizes IBM z/OS UNIX System Services (USS) sockets for cross-address-space communication within an LPAR.

**System security authorizations for RECOVERY MANAGER for DB2**

RECOVERY MANAGER for DB2 requires certain security authorizations.
If you are using RACF or a similar system security package, you must have the following authorizations to use the RECOVERY MANAGER for DB2 product:

- READ authority for archive log data sets
- READ authority for BSDS data sets
- ALTER authority for the DB2 active log data sets
- ALTER authority for the new archive log data sets to be created, if any
- ALTER authority for the archive history file

**DB2 authorizations for RECOVERY MANAGER for DB2**

To use the RECOVERY MANAGER product, you must have the following DB2 authorizations:

- You must have EXECUTE authority on the RMGR plan. (This allows you to build and save an object group and to maintain any object group that you create.)
- To save changes to subsystem default recovery options, you must have one of the following DB2 authorizations:
  - INSTALL SYSADM
  - SYSADM
  - DBADM for the RMGR repository database

**APF authorizations for RECOVERY MANAGER for DB2**

The RMGR load library must be APF-authorized.

In addition, you must add SCCAUTH to the AUTHPGM NAMES section of member IKJTSOxx in SYS1.PARMLIB.

---

**Note**

SCCAUTH is a common authorization module used by multiple BMC Software products, including the components of the BMC Recovery Management for DB2 solution.
Restricting TSO commands for RECOVERY MANAGER for DB2

If your site restricts the use of TSO commands through an option of a RACF or similar system security package, be sure that the ARMUMAN, ARMUSEL, and ARMOPTM command names are added to the appropriate command table. Otherwise, message IKJ5650I ARMUMAN COMMAND NOT FOUND is issued when attempting to invoke the RMGR CLIST.

NGT Recover user authorizations

The BMC Next Generation Technology Recover for DB2 for z/OS product requires certain user authorizations.

DB2 authorizations for BMC Next Generation Technology Recover for DB2 for z/OS

To use the NGT Recover product, you must have the following DB2 authorizations:

■ You must have EXECUTE authority on the NGT Recover plan

  Note
  BMC recommends that you grant the EXECUTE privilege TO PUBLIC for the NGT Recover main plan. This will allow all users to the NGT Recover product.

■ You must have one of the following authorizations:
  — INSTALL SYSADM, SYSADM, or SYSCTRL authority
  — DBADM or DBCTRL authority for the database containing the named spaces
  — RECOVERDB, DISPLAYDB, STARTDB, and STOPDB authority for the databases containing the named table spaces and index spaces

■ If you use NGT Recover to make image copies (OUTCOPY option) from previous image copies, change accumulation files, and DB2 log records, you must have IMAGCOPY authority or an authority that implies IMAGCOPY.

  Note
  If the DB2 Access Control Authorization Exit is being invoked, DB2 authorizations must be granted using Resource Access Control Facility (RACF) or a similar system security package.
**APF authorizations for BMC Next Generation Technology Recover for DB2 for z/OS**

NGT Recover uses system services that require APF authorization.

All load modules loaded by these products must be authorized and must reside in APF-authorized libraries, as follows:

- System sort routine
- IDCAMS
- DSNUTILB

**DASD MANAGER PLUS authorizations**

You can restrict access to the DASD MANAGER PLUS component and the Execution function by controlling the authorization that is granted to these plans.

You can restrict access to the Execution function by using PLAN authorizations.

The names of the plans vary, depending on the version and release of the component that you are using. The conventions for plan names are as follows:

- For DASD MANAGER PLUS: `prdvrDx`
- For Execution: `prdvrDx`

The following table lists the variables for the plan names. An example of a DASD MANAGER PLUS 12.1.00 direct access Report Display plan is ASUC121DR.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>prd</code></td>
<td>Product code</td>
</tr>
<tr>
<td><code>v</code></td>
<td>Version level</td>
</tr>
<tr>
<td><code>r</code></td>
<td>Release level</td>
</tr>
</tbody>
</table>

**Table 76: Plan name variables**
<table>
<thead>
<tr>
<th>Plan name</th>
<th>Function name</th>
<th>Plan description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASUvrDJ</td>
<td>BMCTRIG Utility Job Generation</td>
<td>Controls access to utility-job generation from BMCTRIG. Any user who needs to perform online or BMCTRIG JCL generation should be authorized to use this plan.</td>
</tr>
<tr>
<td>ASUvrDR</td>
<td>Report Display</td>
<td>Controls access to displaying reports. Any user who needs to report events and exceptions online should be authorized to use this plan.</td>
</tr>
<tr>
<td>ASUvrDS</td>
<td>Statistics Collection DB2 Catalog Update Exception, Corrective Action, and Analysis</td>
<td>Controls access to statistics collection and to the operations that update the catalog. Any user who needs to run BMCSTATS or who needs to run BMCTRIG to evaluate objects should be authorized to use this plan.</td>
</tr>
<tr>
<td>ASUvrDZ</td>
<td>Browse DASD MANAGER PLUS Database Statistics</td>
<td>Controls access to the Browse function, which displays statistics from the DASD MANAGER PLUS databases. Any user who needs to display statistics online should be authorized to use this plan. You can restrict the online programs to limit a user to defining objects and specifying and analyzing changes. Consider placing this minimum restriction on the online programs but restricting authorization to run the Execution plans. Doing so allows you to control which users can run changes.</td>
</tr>
<tr>
<td>AEXvrDA</td>
<td>Execution Monitor Entry (Authorization)</td>
<td>Enables users to execute a worklist when EXECUTE authority is granted. You should carefully consider who receives authorization to use this plan.</td>
</tr>
</tbody>
</table>
### Plan name

<table>
<thead>
<tr>
<th>Plan description</th>
<th>Function name</th>
<th>Plan description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEXvrDM (DASD MANAGER PLUS)</td>
<td>Enables users to attach to DB2 with alternate authorization IDs for the -AUTH commands</td>
<td>This plan does not control who has authorization to execute a worklist. Because this plan does not affect who can run Execution, you can grant PUBLIC authority to this plan. The Execution plan contains some packages that use dynamic SQL. Some of these packages cause long-running SQL and might need to be added to your resource limit specification table (RLST). The packages are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ AEXAUNLD unloads data from tables.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ AEXSQLIO performs all worklist -SQL commands, including deletions before a data-only migration -LOAD or -BMCL command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By restricting authorization to run the Execution plans, you can control what change and migrate functions users can perform. The Execution Security Exit provides further control over the Execution component’s authorization switching function.</td>
</tr>
</tbody>
</table>

---

### Enabling data set access

Use one of the following procedures to enable data set access.

**To enable data set access using DB2 RACF ID**

1. In your installation options, specify OPNDB2ID=YES.

   This option tells DASD MANAGER's BMCSTATS utility to use the DB2 RACF ID for data set access.

   **Note**

   Using OPNDB2ID=NO can improve performance. This depends on the size of your data set profiles and on the number of VSAM data sets that are involved in the statistics collection.

**To enable data set access not using the DB2 RACF ID**

1. In your installation options, specify OPNDB2ID=NO.
This option tells DASD MANAGER’s BMCSTATS utility *not* to use the DB2 RACF ID for data set access.

---

2 If you are using RACF or a similar system security package to protect underlying data sets and the Integrated Catalog Facility (ICF) catalog of a table or index space, grant READ privileges for the DB2 VSAM data sets.

### APF authorizations for DASD MANAGER PLUS

DASD MANAGER uses system services that require APF authorization. DASD MANAGER must reside in an APF-authorized library. All load modules loaded by DASD MANAGER must be authorized and must reside in APF-authorized libraries.

### Configuring security for BMC Workbench

This section outlines the security mechanisms for controlling access to BMC Workbench *for DB2* and to IBM DB2.

For further security details, see *BMC Infrastructure Components Administration Guide*.

### Controlling access to BMC Workbench *for DB2*

BMC Workbench *for DB2* provides one plan. The default plan name is BMCGUIPL. This plan is used to perform all BMC Workbench functions and is bound with the CATALOG MANAGER and Common Explain collection IDs.

### Managing DBC security

If you use Computer Technologies CA-ACF2, Computer Technologies CA-Top Secret, or IBM RACF to control access to IBM DB2 you must take into consideration certain requirements.

#### CA-ACF2

If you are using CA-ACF2 to control user access to DB2, you must assign a unique logon ID to the DBC. The logon ID definition must specify the STC option, indicating that the ID is for use by a started task. You must also enable SAF so that CA-ACF2 can recognize the RACROUTE calls that the product issues.
CA-ACF2 can use a TSO command-limiting function to restrict an individual user or an entire site. This function applies to TSO commands that you issue from the READY prompt or from ISPF.

If command limiting is active, you must specify the LGCOMAIN command. The LGCOMAIN command invokes the ISPF interface for the DB2 Product Configuration (LGC) component to allow editing of option sets.

Command limiting can be activated for an individual or an entire site as follows:

- For an individual, with the TSOCMDS field of the logon ID record
  TSOCMDS specifies the name of a module that contains a list of valid commands for a user. For a sample list, see the ACF$CMDS member of CAI.CAIMAC.

- For an entire site, with the CMDLIST field of the GSO record named TSO
  The ALLCMDS field indicates permission for a user to bypass command limiting. Use the character that is specified in the BYPASS field of the GSO TSO record as a prefix for the command name.

**CA-Top Secret**

If you are using CA-Top Secret to control user access to DB2, you must update the Facilities Matrix table to identify the program name. If the program name is not in the table, CA-Top Secret does not allow a program to issue RACROUTE calls. You can specify the first three characters of the program name in the Facilities Matrix table.

**Required grants for CA-ACF2, CA-Top Secret, and RACF**

If you use CA-ACF2 security, define the following grants to CA-ACF2. If you use RACF or CA-Top Secret, define the following grants to DB2:

```
GRANT CREATETAB ON DATABASE BMCPERF
    TO PUBLIC;
GRANT USE OF TABLESPACE BMCPERF.BMCUPLAN
    TO PUBLIC;
```

*Note*

The names in this list of grants reflect the default names used during installation. If you used different names during installation, replace these default names with your own names.

**DB2 security**

To authorize SQL Explains, you can use SYSADM authority or your user ID’s authorization as it exists in DB2. If your user ID does not have Explain authority, you can use the following procedure to allow Explain to acquire SYSADM authority.
This procedure sets the Run authorized (authexpl) option in the GUDOPT option set.

To allow Explain to acquire SYSADM authority

**Note**
Any changes that you make to the Run authorized option affects all users.

1. Invoke the LGCISPF CLIST from the CLIB data set:
   ```
   EX 'HLQ..BMCCLIB(LGCISPF)'
   ```
   If you want to connect to a DBC other than the default DBC, invoke the LGCISPF CLIST with the DBC parm where xxxx is the DBC SSID on that LPAR:
   ```
   EX 'HLQ..BMCCLIB(LGCISPF) 'DBC(xxxx)'
   ```

2. On the DB2 Product Configuration – Main Menu (panel LGCPMENU), select 2 Manage Product Options.

3. In the Product Options Sets panel (LGCP1001), expand the BMC Workbench list by selecting the plus sign (+) next to BMC Workbench and pressing Enter.

4. Type E next to the option set that you want to edit.

5. Set the Run authorized option to Y.

6. Press F3 to save and exit.

### Controlling access to the System and SQL Performance products for DB2

This section outlines the security mechanisms for controlling access to System and SQL Performance products and components and to DB2.

#### User IDs for the DBC component

The DBC is the host address space used by the System and SQL Performance products.

The common Data Collector component for the Performance products runs under the DBC and is sometimes referred to as the DOM agent. The DOM agent is responsible for such things as connecting to DB2 subsystems, starting traces, and collecting and saving data. You can run the DBC as a batch job or as a started task, but BMC recommends running it as a started task. Restrict batch mode to testing the initial installation.
If you plan to use more than one product in the same environment, BMC Software recommends that you use only one DBC for each z/OS image.

The following DBC user IDs are assigned according to the method that was used to start the DBC:

- **Batch**
  The USER parameter of the JOB statement assigns this ID.

- **Started task**
  Your MVS security system assigns this ID based on entries in the equivalent of the RACF ICHRIN03 table. This table contains the name of the started task procedure and the user ID that should be assigned to it. A user ID is often associated with each started task.

  **Note** *(APPTUNE and SQL Performance only)*
  READ authority (or its equivalent) must be granted to the DBC started task ID on SYSUSERAUTH if either of the following conditions are true:
  - DB2 security is being enforced in the DOMPLEX option set through the Security via DB2 authorization table option (see “Verifying or changing the global resource enqueues” on page 246).
  - The DB2 catalog data sets are protected by a security system.
  READ authority (or its equivalent) must be granted to the DBC started task on SYSDBASE if either of the following conditions are true:
  - The object collection is set to Y in the APPTUNE Filter option set.
  - The DB2 catalog data sets are protected by a security system.

Sites frequently allow the security system to assign a default user ID to started tasks so that started tasks can be added without requiring an update to the equivalent of the RACF ICHRIN03 table. In this case, you should grant the necessary authorizations to the user ID of the default started task. If you do not want the products being installed to use this default user ID, you must modify the ICHRIN03 table to assign a different user ID to the DBC.

**Note**
If you make changes to the ICHRIN03 table, an IPL is required to put them into effect.

The user that is assigned to the DBC started task needs RACF authority to the log files. The DOMEXIT1 exit determines the ID that the product uses for DB2 interactions (such as starting traces and executing Explains). Your security system must give this ID permission to perform the operations in DB2. If you did not
customize DOMEXIT1 to use a different ID, the ID that the product uses for DB2
interactions is the default install SYSADM ID for each DB2 subsystem.

Console message IEF695I Procedure procName is assigned to User userID, is issued
at DBC startup, and reports the user ID that the DBC is using. To determine which
user ID the DBC is using, you can also issue the USERS command.

You must also add a rule to provide READ authority to the FACILITY class entity
CSVDYNLN.linkListName when the following conditions exist:

- You are using CA-ACF2, CA-Top Secret, or RACF to control access to DB2.
- You are using LINKLIST instead of STEPLIB for access to the System and SQL
  Performance products.

The linkListName variable represents the name of your LINKLIST data set.

For the authority requirements of the DBC, see “Managing security with CA-ACF2,
CA-Top Secret, or RACF security” on page 109.

Security and permissions for user IDs for the System and
SQL Performance products

Multiple user IDs are associated with installing, configuring, and using the product.

The IDs include:

- Installation user IDs
- DBC started task user IDs
- NGLARCH stated task user IDs
- Online user IDs

For details of the permissions and security settings required by these IDs, see the
BMC Infrastructure Components Administration Guide.

Plan name

The System and SQL Performance products provide one plan. APPTUNE, SQL
Explorer, MainView for DB2 - Data Collector, SQL Performance, and BMC System
Performance use this plan. Pool Advisor does not use a plan.

The default plan name is DAA\vr\D1, where \vr is the version and release level. This
plan is used to perform all SQL Explorer product functions, and for Explains in
APPTUNE, MainView for DB2 - Data Collector, and SQL Performance.
**MVS security**

If you have an MVS security system, you must grant the required authorizations, even if your security system does not control access to DB2.

If you have no MVS security system, see “DB2 and product security” on page 111.

**VSAM data sets**

Table 78 on page 106 describes the function of each data set. For optimum performance, grant global access for each of the following data sets if you are using IBM RACF.

<table>
<thead>
<tr>
<th>Data set</th>
<th>What the data set stores</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE</td>
<td>User Profile user records for all product users and definitions for APPTUNE application groups</td>
</tr>
<tr>
<td></td>
<td>The user record contains the parameters for session characteristics and function keys.</td>
</tr>
<tr>
<td>SECURITY</td>
<td>User Profile security records</td>
</tr>
<tr>
<td></td>
<td>Security records contain parameters that grant or deny access to various product functions and to DB2.</td>
</tr>
<tr>
<td>HELP</td>
<td>Online Help text associated with the products and their components</td>
</tr>
<tr>
<td>COPYDIR</td>
<td>Names of the archived log files for use by the archive directory</td>
</tr>
<tr>
<td>log files</td>
<td>Trace records gathered from DB2 and BMC Software products</td>
</tr>
<tr>
<td>DCC$VARS1</td>
<td>Default parameter variable values and user-coded overrides to variable values (Pool Advisor and System Performance only)</td>
</tr>
<tr>
<td>PMD$HIST</td>
<td>Long-term history records—daily, page sets, and objects (Pool Advisor and System Performance only)</td>
</tr>
</tbody>
</table>

*a* Do not make the name of this data set version sensitive. You retain and reuse these files when you upgrade to a later release of the products.

**Report log data sets (APPTUNE and SQL Performance)**

The installation process does not allocate report log data sets. Users allocate them to store report and screen images for later viewing and printing. See the online Help for information about report logging (HELP TRPTLOG).
**BBPARAM and BBTMPLT data sets**

Although only Pool Advisor and System Performance currently use these data sets, they must be present in order for you to use any of the System and SQL Performance products.

The BBPARAM data set contains the following information:

- Parameters that determine the changes that should be made to the monitored resources and the maximum and minimum threshold values that will be used when advisors recommend changes.
- Rules that trigger recommendations for changes to monitored resources.

The BBTMPLT data set contains the advisor text that is displayed in Pool Advisor and System Performance.

**Data set users**

The following classes of users need authority to access the data sets that the installation process creates:

- DB2 Component Services (DBC)
- Product installer
- Product administrator
  - The product administrator controls internal security and determines whether users should be restricted from performing tasks such as issuing MVS or DB2 commands. A site can designate an individual to be the product administrator or can allow all users to perform administrative functions.
- Product users

Table 79 on page 107 lists RACF access authorization requirements for product data sets and Table 80 on page 108 lists CA-ACF2 access authorization requirements for product data sets. Consult with your security administrator as needed about assigning the appropriate authorizations.

---

**Note**

For more information about DBC security, see “Managing security with CA-ACF2, CA-Top Secret, or RACF security” on page 109.

---

**Table 79: RACF access authorization to product data sets**

<table>
<thead>
<tr>
<th></th>
<th>DBC</th>
<th>Archive processing</th>
<th>Product installer</th>
<th>Product administrator</th>
<th>All users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>NA</td>
<td>NA</td>
<td>A</td>
<td>U</td>
<td>U</td>
</tr>
</tbody>
</table>

User authorizations
### Table 80: CA-ACF2 access to product data sets

<table>
<thead>
<tr>
<th></th>
<th>DBC</th>
<th>Archive processing</th>
<th>Product installer</th>
<th>Product administrator</th>
<th>All users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>R</td>
<td>NA</td>
<td>A</td>
<td>U</td>
<td>R</td>
</tr>
<tr>
<td>Help</td>
<td>NA</td>
<td>NA</td>
<td>A</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Report log</td>
<td>NA</td>
<td>NA</td>
<td>A</td>
<td>U</td>
<td>U&lt;sup&gt;d&lt;/sup&gt;</td>
</tr>
<tr>
<td>Log files</td>
<td>A</td>
<td>R</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Archives</td>
<td>NA</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>COPYDIR</td>
<td>U</td>
<td>U</td>
<td>A</td>
<td>U</td>
<td>R</td>
</tr>
<tr>
<td>PMD$HIST</td>
<td>U&lt;sup&gt;a&lt;/sup&gt;</td>
<td>NA</td>
<td>A&lt;sup&gt;a&lt;/sup&gt;</td>
<td>U&lt;sup&gt;a&lt;/sup&gt;</td>
<td>NA</td>
</tr>
<tr>
<td>DCC$VARS</td>
<td>U&lt;sup&gt;a&lt;/sup&gt;</td>
<td>NA</td>
<td>A&lt;sup&gt;a&lt;/sup&gt;</td>
<td>U&lt;sup&gt;a&lt;/sup&gt;</td>
<td>NA</td>
</tr>
<tr>
<td>BBPARM</td>
<td>R</td>
<td>NA</td>
<td>A</td>
<td>U</td>
<td>NA</td>
</tr>
<tr>
<td>BBTMPLT</td>
<td>R</td>
<td>NA</td>
<td>A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>DB2MSTR</td>
<td>R</td>
<td>NA</td>
<td>R&lt;sup&gt;b&lt;/sup&gt;</td>
<td>R&lt;sup&gt;b&lt;/sup&gt;</td>
<td>R&lt;sup&gt;b&lt;/sup&gt;</td>
</tr>
<tr>
<td>DBC PARMLIB</td>
<td>R</td>
<td>R</td>
<td>A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>DBC repository</td>
<td>A</td>
<td>NA</td>
<td>A</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>DB2 Product Configuration datastore</td>
<td>U&lt;sup&gt;c&lt;/sup&gt;</td>
<td>NA</td>
<td>S</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>RTCS private registry</td>
<td>U</td>
<td>U</td>
<td>A</td>
<td>U</td>
<td>R</td>
</tr>
</tbody>
</table>

Legend: R = READ  U = UPDATE  A = ALTER  S = SUPERUSER  NA = not applicable

- **a** Authorization is required if BMC System Performance or Pool Advisor is installed. Otherwise, authorization is NA.
- **b** The product installer, product administrator, and all users need READ (R) authority if the Data Collector is run with the SECURITY VIA DB2 AUTHORIZATION TABLE option set to Y in the DOMPLEX option set.
- **c** You can use U (UPDATE) if you want to enable users to update their own profile settings or to be able to create their own reports. This access could be set to R (READ) but doing so might cause errors to be displayed. However, you can ignore these messages and the product continues to work normally.
- **d** All users need UPDATE authority to their own report log data sets.

---

**User authorizations**
<table>
<thead>
<tr>
<th>Authorization</th>
<th>DBC</th>
<th>Archive processing</th>
<th>Product installer</th>
<th>Product administrator</th>
<th>All users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>R</td>
<td>NA</td>
<td>WA</td>
<td>W</td>
<td>R</td>
</tr>
<tr>
<td>Help</td>
<td>NA</td>
<td>NA</td>
<td>WA</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Report log</td>
<td>NA</td>
<td>NA</td>
<td>WA</td>
<td>W</td>
<td>W</td>
</tr>
<tr>
<td>Log files</td>
<td>WA</td>
<td>R</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Archives</td>
<td>NA</td>
<td>WA</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>COPYDIR</td>
<td>W</td>
<td>W</td>
<td>WA</td>
<td>W</td>
<td>R</td>
</tr>
<tr>
<td>PMD$HIST</td>
<td>W^a</td>
<td>NA</td>
<td>WA^a</td>
<td>W^a</td>
<td>NA</td>
</tr>
<tr>
<td>DCC$VARS</td>
<td>W^a</td>
<td>NA</td>
<td>WA^a</td>
<td>W^a</td>
<td>NA</td>
</tr>
<tr>
<td>BBPARM</td>
<td>R</td>
<td>NA</td>
<td>WA</td>
<td>W</td>
<td>NA</td>
</tr>
<tr>
<td>BBTMPLT</td>
<td>R</td>
<td>NA</td>
<td>WA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>DB2MSTR</td>
<td>R</td>
<td>NA</td>
<td>R^b</td>
<td>R^b</td>
<td>R^b</td>
</tr>
<tr>
<td>DBC PARMLIB</td>
<td>R</td>
<td>R</td>
<td>WA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>DBC repository</td>
<td>WA</td>
<td>NA</td>
<td>WA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>DB2 Product Configuration datastore</td>
<td>W</td>
<td>NA</td>
<td>S</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>RTCS private registry</td>
<td>W</td>
<td>W</td>
<td>WA</td>
<td>W</td>
<td>R</td>
</tr>
</tbody>
</table>

**Legend:** R = READ  U = UPDATE  A = ALTER  S = SUPERUSER  NA = not applicable

---

**Managing security with CA-ACF2, CA-Top Secret, or RACF security**

If you use CA-ACF2, CA-Top Secret, or RACF to control access to DB2, the following considerations apply.

---

a  Authorization is required if BMC System Performance or Pool Advisor is installed. Otherwise, authorization is NA.

b  The product installer, product administrator, and all users need READ (R) authority if the Data Collector is run with the SECURITY VIA DB2 AUTHORIZATION TABLE option set to Y in the DOMPLEX option set.

c  You can use W (WRITE) if you want to enable users to update their own profile settings or to be able to create their own reports. This access could be set to R (READ) but doing so might cause errors to be displayed. However, you can ignore these messages and the product continues to work normally.
CA-ACF2

If you are using CA-ACF2 to control user access to DB2, you must assign a unique logon ID to the DBC. The logon ID definition must specify the STC option, indicating that the ID is for use by a started task. You must also enable SAF so that CA-ACF2 can recognize the RACROUTE calls that the product issues.

CA-ACF2 can use a TSO command-limiting function to restrict an individual user or an entire site. This function applies to TSO commands that you issue from the READY prompt or from ISPF.

If command limiting is active, you must specify the commands shown in Table 81 on page 110.

**Table 81: Commands you specify in command-limiting environments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMDDMAIN</td>
<td>Access the System and SQL Performance products for DB2 Report Manager for viewing product reports</td>
</tr>
<tr>
<td>BBM9TC21</td>
<td>Hyperlink to the MainView for DB2 component of System Performance</td>
</tr>
<tr>
<td>DMDAIEZ2</td>
<td>Invoke ISPF Edit to allow editing of Pool Advisor for DB2 ZPARM keywords (Pool Advisor and System Performance)</td>
</tr>
<tr>
<td>DMDRJCL1</td>
<td>Invoke ISPF Edit to allow editing of the JCL member created in the Configuration Advisor analysis process (Pool Advisor and System Performance)</td>
</tr>
<tr>
<td>LGCOMAIN</td>
<td>Invoke the ISPF interface for the DB2 Product Configuration (LGC) component to allow editing of option sets</td>
</tr>
<tr>
<td>PSSSQLX</td>
<td>Execute an Explain or a single SQL statement from the product (SQL Explorer, APPTUNE, SQL Performance, and MainView for DB2 – Data Collector)</td>
</tr>
<tr>
<td>PSSDCL</td>
<td>Create a DCLGEN in the product (SQL Explorer and SQL Performance)</td>
</tr>
<tr>
<td>PSSCATI</td>
<td>Invoke common Explain functionality from CATALOG MANAGER for DB2</td>
</tr>
</tbody>
</table>

Command limiting is activated in the following ways:

- For an individual, with the TSOCMDS field of the logon ID record
  TSOCMDS specifies the name of a module that contains a list of valid commands for a user. For a sample list, see the ACF$CMDS member of CAI.CAIMAC.

- For an entire site, with the CMDLIST field of the GSO record named TSO
  The ALLCMDS field indicates permission for a user to bypass command limiting. Use the character that is specified in the BYPASS field of the GSO TSO record as a prefix for the command name.
CA-Top Secret

If you are using CA-Top Secret to control user access to DB2, you must update the Facilities Matrix table to identify the program name. If the program name is not in the table, CA-Top Secret does not allow a program to issue RACROUTE calls. You can specify the first three characters of the program name in the Facilities Matrix table. For the System and SQL Performance products, the first three characters are DOM. These characters then act as a wildcard (DOM*, for example), allowing any program beginning with the characters DOM to issue RACROUTE calls.

CA-ACF2, CA-Top Secret, and RACF

The names in the following list of grants reflect the default names that are used during installation where vr indicates the version and release levels of the product. If you used different names during installation, replace these default names with your own names.

```
GRANT CREATETAB ON DATABASE BMCPERF TO PUBLIC;
GRANT USE OF TABLESPACE BMCPERF.BMCUPLAN TO PUBLIC;
GRANT ALL ON TABLE BMCDAA.vr.SQLX_BASE TO PUBLIC;
GRANT ALL ON TABLE BMCDAA.vr.SQLX_STATS TO PUBLIC;
GRANT ALL ON TABLE BMCDAA.vr.SQLX_SQLTXT TO PUBLIC;
```

Define the grants as follows:

- If you use CA-ACF2 security, define the grants to CA-ACF2.
- If you use RACF or CA-Top Secret, define the grants to DB2.

DB2 and product security

The product administrator is responsible for establishing default security options for all users and for maintaining individual user access options through the User Profile.

The User Profile controls access to the following components and functions:

- Data Collector subsystems
- Authority to issue product commands (through Data Collector subsystems)
- Authority to issue DB2 commands

SECURITY data set and security processing

Product security is enforced through the SECURITY data set. Each user is registered in this data set automatically when a User Profile is created.
Users can modify their User Profiles through User Options or product administrators can modify them in User Profile administration. When a change is made to a User Profile from the administration panels, the records in the PROFILE and SECURITY data sets are updated. When a change is made from the User Options panels, only the record in the PROFILE data set is updated. Administrators can prevent users from modifying many of the profile values by locking the values. Users can view the values in locked fields but cannot modify them. Only users with profile administration authority can change locked values.

When a user begins a product session, the profile records from the SECURITY and PROFILE data sets are merged. If a value is locked, the setting from the SECURITY record is used. If a value is not locked, the setting from the PROFILE data set is used. See the *System and SQL Performance for DB2 Administrator Guide* for a complete description of User Profiles.

**DB2 security**

You can restrict authority to start DB2 traces (APPTUNE and SQL Performance) and issue DB2 commands with product security alone or with DB2 security checking.

Use the DOMPLEX option *Security via DB2 authorization table* to specify the type of security enforcement that the product uses. Specifying N uses only product security (the default), and specifying Y uses both DB2 security and product security:

**Note**

For an explanation of DOMPLEX options, see “Verifying or customizing the DOMPLEX option set” on page 247.

- **Using only product security**
  Authority to issue DB2 commands is controlled exclusively through the product when you specify N for *Security via DB2 authorization table*. This option prevents validation of authorization in DB2. For example, if a User Profile indicates that DB2 commands can be issued, the product allows the user to issue DB2 commands whether or not the user has SYSOPR or other authority in DB2.

  You can use the DOMEXIT2 user exit to override individual security options in the User Profile.

  For more information about DOMEXIT2, see the *System and SQL Performance for DB2 Administrator Guide*.

  For an explanation of DOMPLEX options, see “Verifying or changing DOMPLEX parameters” on page 262.

- **Using both DB2 and product security**
  If you specify Y for *Security via DB2 authorization table*, security is enforced for both DB2 and for the product. For DB2 operations, the product validates authority in the User Profile first. DB2 authority is validated only if the product allows the
operation. For example, if the User Profile indicates that the user is allowed to issue commands, the product validates the user’s DB2 authority. If the user does not have command authorization in DB2, the user cannot issue commands.

On the other hand, because DB2 authorization is checked only if the operation is authorized by the product, it is possible for the product to restrict a user from issuing commands, even when DB2 command authority has been granted to the user. When Y is specified for the Security via DB2 authorization table option, the product can prevent a user from performing a function that DB2 would allow because that function is not authorized by the product. When user access to a specific function is denied because of insufficient security, the product issues error messages.

The product establishes a user’s DB2 authority when the user first logs on to the product. If the target DB2 subsystem is not active when the user logs on, security checking is deferred until DB2 is started and the user makes the first request for a DB2 service.

- **DB2 authorization requirements**

  All product users need DB2 authority. The user assigned to the DBC started task needs RACF authority to the log files and DB2 authority to start traces and execute Explains.

  If you implement a product so that it controls security (by specifying N for the Security via DB2 authorization table option), the product’s User Profile enforces all authorizations when the product is installed. The product’s User Profile also enforces authorization to perform non-DB2-related functions. See “Checking the default User Profile” on page 266 for information about defining a User Profile.

  For detailed information about creating User Profiles, see the System and SQL Performance for DB2 Administrator Guide.

  If you use product security and DB2 security (by specifying Y for the Security via DB2 authorization table option), you must grant the user authorization to the appropriate functions on each DB2 subsystem. You must issue the proper DB2 authority to the user to issue DB2 commands (DISPLAYAUTH for DISPLAY commands and SYSOPRAUTH, SYSADMAUTH, or TRACEAUTH to start and stop traces, for example).

  You must perform these GRANTs before the user begins a product session with a DBC. The user ID that is granted authority in DB2 can be the user ID or, in the TSO environment, a secondary authorization ID within the user’s security group.

  You can use the DOMEXIT4 user exit to override these default user ID selections. This exit is invoked once at the start of each user’s product session. For more information about DOMEXIT4, see the System and SQL Performance for DB2 Administrator Guide.

  The product does not detect the GRANTs and REVOKEs that are issued in a DB2 subsystem until DB2 updates the SYSIBM.SYSUSERAUTH catalog table. If the update is in a DB2 buffer, it might not be written immediately on low-activity DB2 subsystems. If you are using a low-activity DB2 subsystem, you can expedite this update to the catalog table by restarting the DB2 subsystem or by executing the QUIESCE utility against the DSND806.SYSUSER table space. If the product is
executing when a GRANT or REVOKE command is issued, the Data Collector does not recognize the change until you restart the Data Collector or issue a REFRESH command from the Data Collector Command Interface panel or the console.

Log Master *for DB2* user authorizations

To use Log Master, you must have authorization within DB2 and through your system security package (such as the IBM product Resource Access Control Facility or RACF). These authorizations must be sufficient to access DB2 resources and perform the tasks accomplished during processing. The following topics provide more information about the required authorizations.

**DB2 authorizations for Log Master *for DB2***

To ensure that Log Master runs correctly in your environment, you must have the following DB2 authorizations:

- EXECUTE privilege on the Log Master batch and online plans
- DISPLAYDB authority for the databases that contain the named table spaces and index spaces (and any databases related by referential integrity (RI) constraints)
- DISPLAY system privilege
- Authorizations to perform quiesce at log mark
  Before a Log Master job can use this feature of the product, the user ID of the job must also have one of the following DB2 authorizations:
  — DBADM, DBCTL, or DBMAINT authority for the databases
  — SYSCTRL or SYSADM authority
  — IMAGCOPY privilege for the databases
- Authorizations to execute SQL
  Log Master uses the High-speed Apply Engine to execute generated SQL statements. For more details, look for information about DB2 authorizations for High-speed Apply.
  Before a Log Master job can execute SQL, the user ID of the job (or the user ID specified in either the EXECSQL statement or the BINDOWN installation option) must have the following DB2 authorizations:
— EXECUTE privilege for the plan that the High-speed Apply Engine uses to access its own restart tables and the catalog (normally provided during installation)

— EXECUTE privilege for the High-speed Apply Engine restart package (normally provided during installation)

— INSERT, UPDATE, and DELETE privileges on the target tables

— Appropriate privileges to bind or administer plans, packages, and collections

The High-speed Apply Engine provides several ways to grant these privileges. Some techniques avoid granting bind privileges to the user ID that runs Log Master. For more details, look for information about DB2 authorizations for plans, packages, and collections.

**APF authorizations for Log Master for DB2**

To use the Log Master product, you must have the APF authorizations described below.

**APF authorization for batch programs**

Log Master batch programs use operating system services that require APF authorization. Accordingly, the product must reside in APF-authorized libraries. Any libraries that you reference in the STEPLIB DD statements must also be APF-authorized.

**APF authorization for the online interface**

You can run the Log Master online interface with or without APF authorization. The APFONLIN installation option determines whether the product expects to have proper APF authorization.

- Without authorization, an online user must enter the name and location of the bootstrap data set (BSDS) on the Product Options panel. The online interface does not run as an authorized TSO program.

- With proper authorization, the product can obtain the name of the BSDS from DB2 dynamically. The online interface runs as an authorized TSO program.

The TSO program name for the product is SCCAUTH. You must place this name in the operating system’s SYS1.PARMLIB data set in the authorized command table. The command table is a member of SYS.PARMLIB named IKJTSOxx. The suffix xx is assigned during installation. The TSO command table contains several different lists. Place SCCAUTH in the authorized program list (which is specified as AUTHPGM NAMES).
Perform this procedure on all operating system images where you expect the product to run as an authorized TSO program.

RACF authorizations for Log Master for DB2

Log Master for DB2 requires RACF authorizations. Use the method described below to make Log Master work more efficiently in a RACF environment.

Log Master reads data from certain underlying DB2 data sets such as table spaces, active and archive logs, or the bootstrap data set (BSDS). If the underlying data sets are protected by RACF (or by a similar system security package). The user ID of the Log Master batch job must have authority to access all of the underlying data sets that the job requires.

To avoid granting authority for each required data set to the user ID of each Log Master batch job, use the OPNDB2ID installation option. Ensure that all of the following conditions are true:

- Your environment uses RACF.
  The OPNDB2ID installation option does not operate in other security environments.

- You install the product with the OPNDB2ID installation option set to YES.
  When OPNDB2ID is set to YES, Log Master uses the RACF ID of DB2 to open the DB2 data sets.

- You explicitly associate a user ID with the DB2 address space:
  - For OPNDB2ID to work correctly, you must explicitly associate a user ID with DB2 regardless of whether you specify DB2 as a privileged or trusted task in the RACF started procedures table (ICHRIN03).
  - To ensure OPNDB2ID option works correctly in a data sharing environment, the RACF IDs of the DBM1 address spaces within all DB2 subsystems within the data sharing group must be the same. The authorizations for the bootstrap and log data sets must also be the same.

PACLOG for DB2 user authorizations

PACLOG for DB2 requires certain user authorizations.

When all of the following circumstances exist, add ALMUMAN to the list of commands in the TSOCMDS module:
You use the PACLOG logging environment modeling tool.

You use the CA-ACF2 security system.

Your shop restricts TSO commands.

**System security authorizations for PACLOG**

If you are using RACF or a similar system security package, you must have the following authorizations to use the PACLOG product:

- READ authority for archive log data sets
- READ authority for BSDS data sets
- ALTER authority for the DB2 active log data sets
- ALTER authority for the new archive log data sets to be created, if any
- ALTER authority for the archive history file
- DELETE/DEFINE authority for the DB2 archive data sets 1, 2, 3, and 4

**APF authorizations for PACLOG**

To use the PACLOG product, you must have APF authorization for all STEPLIB and JOBLIB libraries.

*Note*

PACLOG does not require an APF-authorized library for installation.

**RACF authorizations for PACLOG**

For RACF security, you must authorize the XCA compression started tasks BMCP and BMCBCSS in the started tasks names table.

**CA-ACF2 authorizations for PACLOG**

For CA-ACF2 security, you must authorize the XCA compression started tasks BMCP and BMCBCSS as started tasks under started task control.

**BMC Archive History File**

The user must have update authority for the BMC Archive History file (an system data set).
R+/CHANGE ACCUM for DB2 user authorizations

R+/CHANGE ACCUM for DB2 requires certain user authorizations.

DB2 authorizations for R+/CHANGE ACCUM

To use the R+/CHANGE ACCUM product, you must have the following DB2 authorizations.

WARNING

SQL access to the repository tables should not be allowed.

Authorizations if using the R+/CHANGE ACCUM batch program

To use the R+/CHANGE ACCUM batch program, R+/CHANGE ACCUM users must have one of the following DB2 authorizations:

- You must have INSTALL SYSADM or SYSADM authority.

- You must have EXECUTE authority on the NGT Recover application plan and one of the following authorizations:
  - SYSCTRL authority
  - DBADM, DBCTRL, DBMAINT, or IMAGCOPY authority for the databases containing the target objects

Authorizations if using the R+/CHANGE ACCUM ISPF interface

To use the R+/CHANGE ACCUM ISPF interface, you must have one of the following authorizations:

- You must have EXECUTE authority for the NGT Recover application plan.

- If you execute the delete change accumulation file function, you must have one of these authorizations:
  - INSTALL SYSADM or SYSADM authority
  - SYSCTRL authority
  - DBADM, DBCTRL, DBMAINT, or IMAGCOPY authority for the databases containing the table spaces that have updates in the file being deleted
**Authorizations if using the MODIFY ACCUM command**

To update the R+/CHANGE ACCUM repository, you must have the same DB2 authorities required to use the R+/CHANGE ACCUM batch program.

**Authorization if deleting change accumulation groups and files**

The R+/CHANGE ACCUM ISPF interface allows users with IMAGCOPY (or equivalent) authority to delete change accumulation groups and files.

To allow a user with INSTALL SYSADM authority to delete change accumulation groups and files, you must specify the user’s ID in the R+/CHANGE ACCUM installation options.

**APF authorizations for R+/CHANGE ACCUM**

R+/CHANGE ACCUM uses system services that require APF authorization. R+/CHANGE ACCUM must reside in an APF-authorized library.

**RACF authorizations for R+/CHANGE ACCUM**

If the archive and active log data sets, the bootstrap data set (BSDS), and the DB2 directory are protected by RACF (Resource Access Control Facility) or by a similar system security package, R+/CHANGE ACCUM users must have READ authority to access the data sets.

---

**Note**

If you are using RACF, and NGT Recover was installed with option OPNDB2ID=YES, the user running NGT Recover does not need READ authority. If your site uses a system security package other than RACF, READ authority is required.

---

**CA-ACF2 authorizations for R+/CHANGE ACCUM**

If you are using CA-ACF2 security with the R+/CHANGE ACCUM product, you must have the following authorizations:

- If your installation uses the “Command Limiting List,” you must add the command processor ACAPRI to the list.

- If the archive and active log data sets, the bootstrap data set (BSDS), and the DB2 directory are protected by CA-ACF2, R+/CHANGE ACCUM users must have READ authority to access the data sets.
Granting user authorizations for EXTENDED BUFFER MANAGER

The XBM security interface allows maximum flexibility in controlling access to XBM functions.

Through the security interface, you can control ISPF access to XBM for a user or a group of users. For example, you can control the ability to change information in the XBM repository and the size of the XBM cache. However, the security interface does not prohibit users from using the ISPF interface to monitor XBM.

You can control access to XBM functions through IBM RACF (version 1.9 or later) or through other security packages that are compatible with the System Authorization Facility (SAF), such as the CA Technologies CA-ACF2 or CA-Top Secret products.

XBM security does not check commands from any MVS system console, including the IBM System Display and Search Facility (SDSF). XBM security checks only commands that are entered through the XBM ISPF interface.

In addition to RACF and other SAF-compatible security packages, the XBM security interface provides two exit points for user-written security routines. For more information, see “Using XBM user exits” on page 127.

The security interface is optional for RACF users and CA-Top Secret users. If you do not implement security access to XBM, its functions are unsecured and available to any user with access to the XBM ISPF interface.

**Note**

If you are using CA-ACF2, the security interface is not optional. By default, CA-ACF2 secures all functions. If you want an unsecured environment, you must implement XBM security and give access to all XBM users, or create an XBM user exit to bypass security checking.

Configuring CA-ACF2 security

You can use CA-ACF2 to secure XBM by defining resource rules for access to XBM functions.

**To configure CA-ACF2 security**

1. Ensure that SAF is enabled on your MVS system.

   XBM issues a RACROUTE macro to SAF to determine whether a request can be approved.
2 Update the INFODIR record as follows:

```
CHANGE INFODIR TYPES(R-RFAC)
```

3 Refresh the INFODIR record.

4 Define resource rules to provide access authority to users of specific XBM actions and resources, by using the following format:

```
$KEY(BMCXBM.ssid.action.object **********)TYPE(FAC)
```

The variables represent the following values:

- **ssid** represents the XBM subsystem ID.
- **action** represents the XBM action.
- **object** represents the XBM object or resource name.

For more information about defining a resource profile, see “RACF resource profiles” on page 122.

5 Rebuild the FAC resource rule by performing an initial program load (IPL) of MVS, or by issuing the following MVS MODIFY command:

```
F ACF2,REBUILD(FAC)
```

For more information about CA-ACF2, see the vendor-provided user documentation for that product.

### Configuring CA-Top Secret security

You can use CA-Top Secret to secure XBM by defining resource profiles for access to XBM functions.

**To configure CA-Top Secret security**

1 Ensure that SAF is enabled on your MVS system.

   XBM issues a RACROUTE macro to SAF to determine if a request can be approved.

2 Add the XBM resource profile BMCXBM and the XBM subsystem (indicated by the **ssid**):

```
TSS ADD(departmentACID) IBMFAC(BMCXBM)
TSS ADD(departmentACID) IBMFAC(ssid)
```

3 Permit access to the XBM resource profile BMCXBM and the XBM subsystem:

```
TSS PER(userID or profile) IBMFAC(BMCXBM.ssid.action.object) ACCESS(Control or higher)
TSS PER(userID or profile) IBMFAC(ssid) ACCESS(UPDATE)
```
Resource profiles for XBM require the following form:

\[ \text{BMCXBM.ssid.action.object} \]

The variables represent the following values:

- \text{ssid} represents the XBM subsystem ID.
- \text{action} represents the XBM action.
- \text{object} represents the XBM object or resource name.

For more information about the XBM resource profile, including values for action and object, see “RACF resource profiles” on page 122. For more information about CA-Top Secret, see the vendor-provided user documentation for that product.

### Configuring RACF security

If you are using the RACF system security package in your system environment, you must have certain authorizations. For more information about RACF, see the IBM RACF documentation.

#### RACF user ID

Installations frequently allow the security system to assign a default user ID to the XBM started tasks.

Consequently, tasks can be added without requiring an update to the equivalent of the RACF ICHRIN03 table. This table contains the name of the started-task procedure and the user ID that should be assigned to it.

If you want to use this method to establish security for the XBM started tasks in your environment, grant started tasks the necessary user ID authorizations. If you do not want XBM to use this default user ID, you must modify ICHRIN03 to assign a different user ID to XBM.

**Note**

If RACF is configured on your MVS system to allow an unknown user, you do not need to supply a user ID for the XBM started task. The XBM started task can run as a RACF unknown user.

#### RACF resource profiles

To secure XBM functions by using RACF security, you should use one or more RACF resource profiles that are defined with a class of `Facility`. 
A facility-class resource profile lets you protect your nonstandard resources, such as program actions. These resource profiles let you control access to one or more resources with similar names and identical security requirements and protect a group of related resources.

**Note**

Each user or group that is given access to an XBM RACF resource profile must have an access level of **Control** or higher.

Define a RACF resource profile as follows:

\[ \text{BMCXBM.ssid.action.object} \]

The variables represent the following values:

- **BMCXBM** specifies that the profile is for XBM.
- **ssid** represents the name of the XBM subsystem.
- **action** represents the XBM function to be secured.
- **object** represents the XBM object or resource name to be secured.

Wildcard patterns are supported for **ssid**, **action**, and **object**, according to RACF rules.

The following table defines the values for **action** and **object**:

<table>
<thead>
<tr>
<th>Action</th>
<th>Object</th>
<th>Action description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN</td>
<td>CONFIG</td>
<td>Activates a configuration</td>
</tr>
<tr>
<td></td>
<td>MS</td>
<td>Activates or deactivates a management set</td>
</tr>
<tr>
<td>COPY</td>
<td>EMCSYMM</td>
<td>Splits a Business Continuance Volume (BCV) device</td>
</tr>
<tr>
<td></td>
<td>PPRC</td>
<td>Splits a Peer-to-Peer Remote Copy (PPRC) device</td>
</tr>
<tr>
<td>MAINT</td>
<td>CONFIG</td>
<td>Adds, updates, deletes, or renames a configuration</td>
</tr>
<tr>
<td></td>
<td>MS</td>
<td>Adds, updates, deletes, or renames a management set</td>
</tr>
<tr>
<td></td>
<td>OPTION</td>
<td>Changes XBM, IMS, PSS, SSI, and VSAM options</td>
</tr>
<tr>
<td>PROTECT</td>
<td>EMCSYMM</td>
<td>Controls the hold or release of a BCV device</td>
</tr>
<tr>
<td>RESET</td>
<td>DATASET</td>
<td>Resets data set statistics</td>
</tr>
<tr>
<td>RESTORE</td>
<td>EMCSYMM</td>
<td>Restores or incrementally restores a standard volume from a BCV</td>
</tr>
<tr>
<td>SNAP</td>
<td>DATASET</td>
<td>Controls Instant Snapshot support for utility jobs</td>
</tr>
<tr>
<td></td>
<td>VOLUME</td>
<td>Controls hardware snapshot support for virtual volumes</td>
</tr>
<tr>
<td>Action</td>
<td>Object</td>
<td>Action description</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSIALLOW</td>
<td>LMIRROR</td>
<td>Controls the SSI option to make local mirrors available for EMC SRDF snapshots</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMIRROR</td>
<td></td>
<td>Controls the SSI option to make remote mirrors available for EMC SRDF snapshots</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYNC@REG</td>
<td></td>
<td>Controls the SSI option to synchronize EMC BCVs at snapshot registration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYNC</td>
<td>EMCSYMM</td>
<td>Establishes or reestablishes a BCV from a standard volume</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PPRC</td>
<td>Establishes or reestablishes a PPRC volume from a standard volume</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYSTEM</td>
<td>COMPONENT</td>
<td>Starts or stops the XBM, DB2, IMS, PSS, SSI, and VSAM components</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SENDCMD</td>
<td>Explicitly or implicitly issues the XBM SEND command to communicate with a utility job that is connected to the utility monitor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIMULATE</td>
<td>Sets simulate mode (not supported for snapshot processing)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>STOPXBM</td>
<td>Terminates XBM processing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNAPSHOT</td>
<td>Runs jobs that use XBM snapshot utilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UTILJOB</td>
<td>Connects to the utility monitor (for users of snapshot utilities)</td>
</tr>
<tr>
<td>ZIIP</td>
<td></td>
<td>Uses zIIP feature</td>
</tr>
</tbody>
</table>

**Examples of RACF resource profiles**

- **Controlling access to XBM maintenance actions**

  The following example shows how you can control access to *all* XBM maintenance actions for configurations (add, update, rename, and delete) on an XBM subsystem named XBMP:

  ```
  BMCXBMB.XBMP.MAINT.CONFIG
  ```

  To control access to all XBM maintenance actions for configurations, management sets, and options, use the following profile:

  ```
  BMCXBMB.XBMP.MAINT.*
  ```

- **Controlling access to all XBM subsystems and actions**

  To control access to all XBM subsystems and all XBM actions (ADMIN, MAINT, and SYSTEM) for all XBM resources, use the following profile:

  ```
  BMCXBMB.*.*.*
  ```

  When XBM is started as a job or a started task, it activates a configuration. If you are using the security interface, XBM must be in the RACF started-task table and must have an associated RACF user ID.
Controlling access to intelligent storage manipulation

To control access to intelligent storage manipulation (split and establish storage device mirrors) on an XBM subsystem, use the following profiles:

- BMCXB.MXBMP.COPY.* (to control mirror split)
- BMCXB.MXBMP.SYNC.* (to control mirror establish)

**Note**

These actions must be available to the user ID of any snapshot jobs that are expected to use SSI-enabled hardware features, such as hardware snapshots or Instant Snapshots. Otherwise, limit access to users who are expected to manipulate intelligent storage features.

Controlling access to virtual volume snapshots

If you enable virtual volume snapshots, you should define a resource profile as follows:

- BMCXB.ssid.SNAP.VVOLUME

In this profile, ssid indicates the XBM subsystem. SNAP and VVOLUME indicate the function and object to be secured.

No RACF authorization by default

If you are running MVS with no RACF authorization by default, you must authorize the following resource profiles to the XBM started task.

At a minimum, the XBM started task requires authorization to these resource profiles to successfully initialize:

- BMCXB.ssid.MAINT.CONFIG
- BMCXB.ssid.ADMIN.CONFIG

The variable ssid represents the name of the XBM subsystem.

**Note**

Any user or group that has access to the resource profile must have an access level of Control or higher, and these profiles must be defined with a class of Facility. This class of profile will enable you to protect your nonstandard resources, such as program actions.

RACF resource profiles

To secure XBM functions by using RACF security, you should use one or more RACF resource profiles that are defined with a class of Facility.

A facility-class resource profile lets you protect your nonstandard resources, such as program actions. These resource profiles let you control access to one or more...
resources with similar names and identical security requirements and protect a
group of related resources.

**Note**

Each user or group that is given access to an XBM RACF resource profile must have
an access level of **Control** or higher.

Define a RACF resource profile as follows:

```
BMCXBM.ss.id.action.object
```

The variables represent the following values:

- **BMCXBM** specifies that the profile is for XBM.
- **ssid** represents the name of the XBM subsystem.
- **action** represents the XBM function to be secured.
- **object** represents the XBM object or resource name to be secured.

Wildcard patterns are supported for **ssid**, **action**, and **object**, according to RACF
rules.

Table 82 on page 123 defines the values for **action** and **object**.

**Table 83: Security action and object values**

<table>
<thead>
<tr>
<th>Action</th>
<th>Object</th>
<th>Action description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN</td>
<td>CONFIG</td>
<td>Activates a configuration</td>
</tr>
<tr>
<td></td>
<td>MS</td>
<td>Activates or deactivates a management set</td>
</tr>
<tr>
<td>COPY</td>
<td>EMCSYMM</td>
<td>Splits a Business Continuance Volume (BCV) device</td>
</tr>
<tr>
<td></td>
<td>PPRC</td>
<td>Splits a Peer-to-Peer Remote Copy (PPRC) device</td>
</tr>
<tr>
<td>MAINT</td>
<td>CONFIG</td>
<td>Adds, updates, deletes, or renames a configuration</td>
</tr>
<tr>
<td></td>
<td>MS</td>
<td>Adds, updates, deletes, or renames a management set</td>
</tr>
<tr>
<td></td>
<td>OPTION</td>
<td>Changes XBM, IMS, PSS, SSI, and VSAM options</td>
</tr>
<tr>
<td>PROTECT</td>
<td>EMCSYMM</td>
<td>Controls the hold or release of a BCV device</td>
</tr>
<tr>
<td>RESET</td>
<td>DATASET</td>
<td>Resets data set statistics</td>
</tr>
<tr>
<td>RESTORE</td>
<td>EMCSYMM</td>
<td>Restores or incrementally restores a standard volume from a BCV</td>
</tr>
</tbody>
</table>
### Using XBM user exits

XBM provides the ability for your installation to write either or both of the following security exits: XBMXAEX1 and XBMXAEX2. You can use these exits to provide security for installations without an SAF-compatible security package, or you can use them to supplement an SAF-compatible security package.

If the exit routines are in your XBM load library, XBM calls the routines. You can pass parameters to these exits by using the standard ALC conventions.

#### XBMXAEX1 exit

XBM calls the XBMXAEX1 exit after XBM gets the user ID.

The exit passes a pointer to a copy of the user ID. The copied user ID is eight characters long. If required, the user ID is padded with blanks.
You can use this exit to change the user ID in any way, because you are changing only what XBM sees as a user ID. XBM does not check any return codes.

**XBMXAEX2 exit**

XBM calls the XBMXAEX2 exit when a user attempts to perform any of the protected action and object pairs.

“RACF resource profiles” on page 122 describes the protected action and object pairs.

XBM passes the following parameters to this exit:

- A pointer to the user ID, which the XBMXAEX1 exit might have modified
  The user ID is eight characters. If required, the user ID is padded with blanks.

- A pointer to the fully qualified `action.object`
  This parameter is variable in length and is delimited by a null (X'00').

For example, if the user is trying to activate a configuration on XBMP, the second parameter points to the following string of characters:

```plaintext
BMCXBM.XBMP.ADMIN.CONFIG
```

A null (X'00') immediately follows the character string.

The exit returns a return code. You can use this exit to pass a return code to XBM that can result in bypassing any further security checking.

The following table describes the required return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Authorized and no security checking is required</td>
</tr>
<tr>
<td>4</td>
<td>Ignore and perform security checking</td>
</tr>
<tr>
<td>8</td>
<td>No authority</td>
</tr>
</tbody>
</table>

**High-speed Apply Engine user authorizations**

High-speed Apply Engine requires certain user authorizations.
**DB2 authorizations for the High-speed Apply Engine**

The High-speed Apply Engine requires certain DB2 authorizations to run correctly.

To execute SQL or logical log input, the user ID that runs the High-speed Apply Engine must have the following DB2 authorizations:

- EXECUTE privilege for the plan that High-speed Apply uses to access its own restart tables and the catalog
- EXECUTE privilege for the restart package
- Appropriate table privileges such as, INSERT, UPDATE, or DELETE for the target tables (the specific privileges depend on the actions that the apply request performs)
- Appropriate privileges to bind or administer plans, packages, and collections

High-speed Apply provides several ways to grant these privileges. Some techniques avoid granting bind privileges to the user ID that runs High-speed Apply. For more information, see the topic on DB2 authorizations for plans, packages, and collections.

**DB2 authorizations for the plans, packages, and collections of the High-speed Apply Engine**

The High-speed Apply Engine creates plans, packages, and collections. Depending on the privileges that you are willing to grant to the user ID that runs High-speed Apply Engine, you can grant the DB2 authorizations and privileges for these activities using one of the methods described in this section.

The following table defines the variables that appear in all of the GRANT examples in this section. For more information about the parameters discussed in this section, see the *High-speed Apply Engine Reference Manual*.

<table>
<thead>
<tr>
<th>Table 85: Variables used in DB2 authorization examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Variable name</strong></td>
</tr>
<tr>
<td>aptPlan</td>
</tr>
<tr>
<td>Variable name</td>
</tr>
<tr>
<td>---------------</td>
</tr>
</tbody>
</table>
| collectionIDs | Names of collections to which High-speed Apply Engine dynamically binds packages during processing. This name can be one of the following:  
- One specific package designated for use by High-speed Apply Engine  
- List of specific packages designated for use by High-speed Apply Engine  
- "*"  
  This wild card represents all collections. Your security policies might not permit this specification. |
| databaseName | Target database being changed by the apply request |
| tableName | Target tables being changed by the apply request |
| userID01 | Authorization ID of the user running the apply request. You can specify PUBLIC or a specific authorization ID. |
| userID02 | Authorization ID (different than userID01) with authority to bind plans, bind packages, and administer collections. This authorization ID can be a secondary authorization ID. The privileges that are granted to this authorization ID vary, depending on how you enable High-speed Apply Engine bind processing. |
| userPlan01 | Name of a pre-bound plan that is bound by using special bind options (optional, when the BindAction parameter is Use) |

**Using the user ID running High-speed Apply for authorizations**

With this method, you must grant authority and privileges to the user ID running the High-speed Apply Engine. This method has the following requirements:

- The user ID that runs High-speed Apply Engine (userID01) must have BINDADD authority, and one of the following statuses:
  - PACKADM authority
  - CREATE privileges on all packages ("")
  - CREATE privileges on a specific collection or list of collections designated for use by High-speed Apply Engine
- If userID01 has CREATE privileges only on specific collections, the apply request must specify one of those collection names as the value of the CollectionID parameter.
Authorization examples for the user ID running High-speed Apply Engine

The following examples show the grant actions that are normally done during and after installation. The authorizations that you grant depend on your own security policies. For definitions of the variables shown in these examples, see the preceding table.

---

**Example**

This example shows the authorizations that provide access to the High-speed Apply plan and restart table. These authorizations are normally granted during installation.

```sql
GRANT EXECUTE ON PLAN aptPlan TO userid01;
GRANT EXECUTE ON PACKAGE BMCAPT.APTREB2 TO userid01;
```

---

**Example**

This example shows additional authorizations that are required to run the High-speed Apply Engine. These authorizations are normally granted after installation.

```sql
GRANT INSERT, UPDATE, SELECT, DELETE ON tableNames TO userid01;
GRANT BINDADD TO userid01;
GRANT PACKADM ON COLLECTION collectionIDs TO userid01;
or
GRANT CREATE ON COLLECTION collectionIDs TO userid01;
```

---

### Using BindOwner and a pre-bound plan

With this method, High-speed Apply Engine uses a pre-bound plan that was created under the authority of a different user ID. The pre-bound plan is validated at run time; therefore, it must have been previously bound by a different user ID with appropriate privileges. For a sample BIND command, see the *High-speed Apply Engine Reference Manual*.

This method has the following requirements:

- The user ID that runs High-speed Apply (*userId01*) must have
  - EXECUTE privilege on a specific pre-bound plan
  - BINDAGENT authority

- To be validated at run time, the plan must have been previously bound by a different user ID (*userId02*) with appropriate privileges.

- *userId02* must have BINDADD authority and one of the following statuses:
— PACKADM authority

— CREATE privileges on all packages (*)

— CREATE privileges on a specific collection or list of collections that is designated for use by High-speed Apply

The apply request must specify the following parameter values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BindAction</td>
<td>Use</td>
</tr>
<tr>
<td>BindOwner</td>
<td>User ID that bound the plan</td>
</tr>
<tr>
<td>CollectionID</td>
<td>Name of the High-speed Apply Engine collection</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This value is required if the user ID that binds the plan has CREATE privileges only on specific collections.</td>
</tr>
<tr>
<td>PlanName</td>
<td>Name of the specific prebound plan</td>
</tr>
</tbody>
</table>

**Authorization examples for using a pre-bound plan**

The following examples show the authorizations that are normally granted during and after installation. The authorizations that you grant depend on your own security policies. For definitions of the variables shown in these examples, see the table at the beginning of this topic.

This example shows the authorizations that provide access to the High-speed Apply plan and restart table. These authorizations are normally granted during installation.

```sql
GRANT EXECUTE ON PLAN aptPlan TO userid01;
GRANT EXECUTE ON PACKAGE BMC.APTREB2 TO userid01;
```

This example shows additional authorizations that are required to run the High-speed Apply Engine. These authorizations are normally granted after installation.

```sql
GRANT INSERT, UPDATE, SELECT, DELETE ON tablesNames TO userid01;
GRANT EXECUTE ON PLAN userPlan01 TO userid01;
GRANT BINDAGENT TO userid01;
GRANT BINDADD TO userid02;
GRANT PACKADM ON COLLECTION collectionIDs TO userid02;
or
GRANT CREATE ON COLLECTION collectionIDs TO userid02;
```
Using the AuthID parameter

With this method, High-speed Apply Engine binds by using the authority of a specified user ID. High-speed Apply Engine uses this user ID only for bind processing. This method has the following requirements:

- The user ID that runs High-speed Apply Engine (userid01) must have EXECUTE privilege for the High-speed Apply Engine plan and restart table package. This user ID does not require special privileges for bind actions.

- The user ID that you specify for bind processing (userid02) can be a primary or secondary authorization ID, and
  - Must have SYSADM authority or SYSCTRL authority
  - Must be a valid TSO logon ID; otherwise, your security software can issue warning messages or prevent required processing
  - Cannot be a group ID

- The apply request must specify userid02 as the value of the AuthId configuration parameter.

Authorization examples for using the AuthID parameter

The following examples show the authorizations that are normally granted during and after installation. The authorizations that you grant depend on your own security policies. For definitions of the variables shown in these examples, see the table at the beginning of this topic.

Example

This example shows the authorizations that provide access to the High-speed Apply Engine plan and restart table. These authorizations are normally granted during the install process.

```
GRANT EXECUTE ON PLAN aptPlan TO userid01;
GRANT EXECUTE ON PACKAGE BMCAPT.APTREB2 TO userid01;
```
Example

This example shows additional authorizations that are required to run the High-speed Apply Engine. These authorizations are normally granted after installation.

```sql
GRANT INSERT, UPDATE, SELECT, DELETE ON tableNames TO userid01;
GRANT SYSADM TO userid02;
or
GRANT SYSCTRL TO userid02;
```

Summary of DB2 authorization requirements for the High-speed Apply Engine

The following table summarizes the DB2 authorizations requirements for different methods of specifying the [Bind] parameters to run High-speed Apply Engine. Note the following authorization considerations:

- Though any of the listed DB2 authorizations or privileges can be granted to PUBLIC, many of them normally are not; for example, SYSADM, SYSCTRL, BINDADD, and PACKADM.

- The BindOwner value must be one of the following:
  - A valid primary or secondary authorization ID of the user running High-speed Apply Engine
  - An authorization ID (with sufficient authority) that has granted BINDAGENT authority to the user running High-speed Apply Engine

- The AuthID value:
  - Must be a valid TSO logon ID, not a group ID
  - Does not have to be a valid secondary authorization ID of the user running High-speed Apply Engine
Table 86: Summary of DB2 authorization requirements for High-speed Apply Engine

<table>
<thead>
<tr>
<th>[Bind] parameter usage</th>
<th>DB2 authorization</th>
<th>Granted to one of listed IDs or to PUBLIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default [Bind] parameters (if you do not specify any parameters in your configuration)</td>
<td>EXECUTE privilege for High-speed Apply Engine plan (for example, APTBvvr)</td>
<td>■ Primary authorization ID (user ID)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Secondary authorization ID</td>
</tr>
<tr>
<td></td>
<td>EXECUTE privilege for restart table package (for example, APTBvvr.APTREB2)</td>
<td>Primary authorization ID (user ID)</td>
</tr>
<tr>
<td></td>
<td>BINDADD authority</td>
<td>Primary authorization ID (user ID)</td>
</tr>
<tr>
<td></td>
<td>PACKADM authority or CREATE IN privilege for collection</td>
<td>Primary authorization ID (user ID)</td>
</tr>
<tr>
<td></td>
<td>SELECT, INSERT, UPDATE, and DELETE privileges on target tables</td>
<td>Primary authorization ID (user ID)</td>
</tr>
<tr>
<td>Specify value for BindOwner (APOWNER) parameter</td>
<td>EXECUTE privilege for High-speed Apply Engine plan (for example, APTBvvr)</td>
<td>■ Primary authorization ID (user ID)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Secondary authorization ID</td>
</tr>
<tr>
<td></td>
<td>EXECUTE privilege for restart table package (for example, APTBvvr.APTREB2)</td>
<td>Authorization ID specified by BindOwner parameter</td>
</tr>
<tr>
<td></td>
<td>BINDADD authority</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PACKADM authority or CREATE IN privilege for collection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SELECT, INSERT, UPDATE, and DELETE privileges on target tables</td>
<td></td>
</tr>
<tr>
<td>Specify value for AuthID parameter</td>
<td>EXECUTE privilege for High-speed Apply Engine plan(for example, APTBvvr)</td>
<td>■ Primary authorization ID (user ID)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Secondary authorization ID</td>
</tr>
<tr>
<td></td>
<td>EXECUTE privilege for restart table package (for example, APTBvvr.APTREB2)</td>
<td>Primary authorization ID (user ID)</td>
</tr>
<tr>
<td></td>
<td>SYSADM or SYSCTRL authority</td>
<td>Authorization ID specified by AuthID parameter</td>
</tr>
<tr>
<td></td>
<td>SELECT, INSERT, UPDATE, and DELETE privileges on target tables</td>
<td>Primary authorization ID (user ID)</td>
</tr>
<tr>
<td>[Bind] parameter usage method</td>
<td>DB2 authorization</td>
<td>Granted to one of listed IDs or to PUBLIC</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------</td>
</tr>
</tbody>
</table>
| Specify value for AuthID and BindOwner (APOWNER) parameters | EXECUTE privilege for High-speed Apply Engine plan (for example, APTB vvr) | • Primary authorization ID (user ID)  
• Secondary authorization ID |
| | EXECUTE privilege for restart table package (for example, APTB vvr:APTREB2) | Authorization ID specified by BindOwner parameter |
| | SYSADM or SYSCTRL authority | Authorization ID specified by AuthID parameter |
| | SELECT, INSERT, UPDATE, and DELETE privileges on target tables | Authorization ID specified by BindOwner parameter |

**APF authorizations for the High-speed Apply Engine**

To use the High-speed Apply Engine, you must have the following APF authorizations:

- The High-speed Apply load libraries must be APF-authorized.

- Any libraries you reference in the apply request (in the STEPLIB DD statements) must be APF-authorized.

The user ID that submits the apply request must have the appropriate authorizations to run the request.

**NGT data set access and security settings**

The system administrator should use the following tables to assign the appropriate security settings for the designated role of the user.

**Table 87: Installer role**

<table>
<thead>
<tr>
<th>Library</th>
<th>Access required</th>
</tr>
</thead>
</table>
| yourNGT_LOAD  | • ALLOCATE/ALTER  
• UPDATE  
• READ  
• EXECUTE |
### Table 88: All other roles

<table>
<thead>
<tr>
<th>Library</th>
<th>Access required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>yourNGT.CNTL</code></td>
<td>- ALLOCATE/ALTER&lt;br&gt;                              - UPDATE&lt;br&gt;- READ&lt;br&gt;- EXECUTE</td>
</tr>
<tr>
<td><code>yourNGT.LOGPDS</code></td>
<td>- ALLOCATE/ALTER&lt;br&gt;- UPDATE&lt;br&gt;- READ</td>
</tr>
<tr>
<td><code>yourNGT.CKPT1001</code></td>
<td>- ALLOCATE/ALTER&lt;br&gt;- UPDATE&lt;br&gt;- READ</td>
</tr>
</tbody>
</table>

### Table 89: NGT Subsystem (CDBSS)

<table>
<thead>
<tr>
<th>Library</th>
<th>Access required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>yourNGT.CNTL</code></td>
<td>- READ&lt;br&gt;- EXECUTE</td>
</tr>
<tr>
<td><code>yourNGT.LOGPDS</code></td>
<td>- UPDATE&lt;br&gt;- READ</td>
</tr>
<tr>
<td><code>yourNGT.CKPT1001</code></td>
<td>- UPDATE&lt;br&gt;- READ</td>
</tr>
<tr>
<td><code>yourNGT.Load</code></td>
<td>- UPDATE&lt;br&gt;- READ&lt;br&gt;(If the user needs authority to configure utility products)&lt;br&gt;- READ&lt;br&gt;- EXECUTE</td>
</tr>
</tbody>
</table>
Some systems may have ACF2/RACF rules already in place that will accommodate the NGT utility products. For example, if SYS2 data sets have READ and EXECUTE access for everyone and SYS3 data sets have READ, EXECUTE, and also UPDATE access for everyone. If this is the case, then NGT Load could be installed as SYS2.yourNGT:LOAD, yourNGT:CNTL could be installed as SYS2.yourNGT:CNTL, yourNGT:LOGPDS could be installed as SYS3.yourNGT:LOGPDS, and yourNGT.CKPT001 could be installed as SYS3.yourNGT.CKPT001.

### NGT authorizations

The NGT utilities require certain user authorizations.

#### DB2 Plan Authorizations

The system administrator should grant EXECUTE authority on the NGT utility products plan to those users that will be running a NGT utility product. All DB2 utility authorizations are checked by NGT at runtime. Secondary authorization IDs are supported.

NGT utility products require the following minimum access privileges are present before allowing execution. SYSADM and SYSCTL levels have all required accesses.

<table>
<thead>
<tr>
<th>Utility Product</th>
<th>VSAM authority</th>
<th>Minimum DB2 authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGT Copy</td>
<td>READ</td>
<td>IMAGCOPYAUTH</td>
</tr>
<tr>
<td>NGT Load</td>
<td>ALTER</td>
<td>LOADAUTH</td>
</tr>
<tr>
<td>NGT Reorg</td>
<td>ALTER</td>
<td>REORGAUTH</td>
</tr>
<tr>
<td>REORG INDEX</td>
<td>ALTER</td>
<td>REORGAUTH</td>
</tr>
<tr>
<td>NGT Unload</td>
<td>READ</td>
<td>IMAGCOPYAUTH</td>
</tr>
<tr>
<td>UNLOAD SHRLEVEL CHANGE</td>
<td>READ</td>
<td>SELECTAUTH</td>
</tr>
<tr>
<td>NGT Stats</td>
<td>UPDATE</td>
<td>Authorization not checked</td>
</tr>
<tr>
<td>REBUILD INDEX</td>
<td>ALTER</td>
<td>Authorization not checked</td>
</tr>
</tbody>
</table>

The VSAM authority must be held by the individual running the NGT utility products or by the userids specified in the global parameter +RACFID. For an explanation of +RACFID, see the BMC Next Generation Technology General User Guide.
**APF Authorization**

The `UserHLQ.UBMCLINK` data set must be APF-authorized.

The `UserHLQ.UBMCLINK` data set, together with the `UserHLQ.UBMCCNTL` and `UserHLQ.UBMCAUTO` data sets are created during the installation process.

To update the APF list, on any MVS console issue the following command:

```
SETPROG APF,ADD,DSNAME=LIBRARY,VOLUME=volume
```

**Required authorizations for NGT Check**

Using NGT Check requires the following authorizations:

- On the database, COPY authority
- For the user, SYSADM authority or DBADM authority

**Required authorizations for NGT Reorg**

NGT Reorg requires the following authorizations:

- REORG authority on the database
- SYSADM or DBADM authority

**Required authorizations for NGT LOBMaster**

LOBMaster requires one of the following authorizations:

- REORG authority on the database
- SYSADM or DBADM authority

**Required authorizations for NGT Reorg**

NGT Reorg requires the following authorizations:

- REORG authority on the database
- SYSADM or DBADM authority

**Required authorizations for NGT Stats**

NGT Stats requires the following authorizations:

- For the database, STATS authority
- One of the following administrator authorities:
Required authorizations for NGT Unload

Using NGT Unload requires the following authorizations:

- One of the following for the database:
  - SYSADM
  - DBADM
  - COPY

- One of the following for the tables:
  - Ownership
  - SELECT
  - SYSCTRL (catalog tables only)

Restricting access to the worklist parallelism feature

The Database Administration solution enables you to use the worklist parallelism feature to run portions of a CHANGE MANAGER worklist concurrently. CHANGE MANAGER uses the XIM technology to provide sysplex performance improvements by enabling the distribution and management of discrete units of work (UOW) across one or more IBM OS/390 and z/OS images.

By default, user access to execute portions of a worklist concurrently and to dynamically start XIM is not restricted. You can control access to these functions for a user or a group of users by performing the following tasks:

1. Apply a zap.
2. If you are using RACF, specify a general resource profile.

Note
If you are using another security package that is compatible with the System Authorization Facility (SAF), contact Customer Support.
To apply a zap

1. To enable the restriction of access to these functions, apply the following zap to the Execution function of CHANGE MANAGER:

   NAME  AEXPMAIN MAINRACC
   VER  003E 47F0.C1D8
   REP  003E 4700,0000
   CHECKSUM 0916482E

To specify a general resource profile

In RACF, general resource profiles are used to protect the resources that are defined in the class descriptor table, such as programs.

1. To restrict a user’s or group’s access to each of the worklist parallelism functions, you must add general resource profiles with the following profile information:

   ■ CLASS => FACILITY
   ■ PROFILE => BMCACM.ssid.PARALLEL.objectName

   The profile definition contains the following values:

   ■ BMCACM specifies that the profile is for CHANGE MANAGER.

   ■ ssid represents the name of the DB2 subsystem or a DB2 group attachment name (wildcard characters can be used to match one or more characters).

   ■ PARALLEL represents the function that is secured.

   ■ objectName represents the object or resource name that is secured.

      — For executing a worklist, the objectName is EXECUTE.

      — For starting XIM dynamically, the objectName is DYNSTART.

   Each user or group that is given access to a resource profile must have an access level of CONTROL or higher.
System-level changes

This chapter describes customization tasks that are required for specific products, and affect the system.

Setting the MEMLIMIT system parameter

Several BMC products require above-the-bar memory and might abend if sufficient memory is not available. This requirement affects the BMC products and solutions listed in the table in this section.

The default value for the System Management Facility (SMF) MEMLIMIT parameter is 2 GB. This value is set in member SMFPRMxx in SYS1.PARMLIB.

Before you begin

Determine whether you need to override the default MEMLIMIT value, based on the information in the following table:

<table>
<thead>
<tr>
<th>Product or solution</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Assistant</td>
<td>If you are unable to specify REGION=0M:</td>
</tr>
<tr>
<td></td>
<td>▪ Specify NOLIMIT to allow unlimited above-the-bar memory.</td>
</tr>
<tr>
<td></td>
<td>▪ If you are unable to specify NOLIMIT, specify at least 4 GB; if you are</td>
</tr>
<tr>
<td></td>
<td>operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>ALTER</td>
<td>If you are unable to specify REGION=0M, specify at least 1 GB; if you are</td>
</tr>
<tr>
<td></td>
<td>operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>CATALOG MANAGER</td>
<td>If you are unable to specify REGION=0M, specify at least 1 GB; if you are</td>
</tr>
<tr>
<td></td>
<td>operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>Product or solution</td>
<td>Recommendation</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>CHANGE MANAGER</td>
<td>If you are unable to specify REGION=0M, specify at least 1 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
</tbody>
</table>
| CHECK PLUS         | If you are unable to specify REGION=0M:  
  - Specify NOLIMIT to allow unlimited above-the-bar memory.  
  - If you are unable to specify NOLIMIT, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB. |
| NGT Copy           | Specify at least 2 GB, if you are operating on LOB or XML data, BMC recommends at least 32 GB. |
| DASD MANAGER PLUS  | If you are unable to specify REGION=0M:  
  - Specify NOLIMIT to allow unlimited above-the-bar memory.  
  - If you are unable to specify NOLIMIT and above-the-bar memory limits are inadequate, contact your z/OS system administrator. |
| Database Administration | If you are unable to specify REGION=0M:  
  - Specify NOLIMIT to allow unlimited above-the-bar memory.  
  - If you are unable to specify NOLIMIT, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB. |
| Database Performance | If you are unable to specify REGION=0M:  
  - Specify NOLIMIT to allow unlimited above-the-bar memory.  
  - If you are unable to specify NOLIMIT:  
    - For DASD MANAGER, if above-the-bar memory limits are inadequate, contact your z/OS system administrator.  
    - For REORG PLUS, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB. |
| High-speed Apply Engine | Specify at least 1 GB. |
| BMC High Speed Utilities for DB2 | If you are unable to specify REGION=0M:  
  - Specify NOLIMIT to allow unlimited above-the-bar memory.  
  - If you are unable to specify NOLIMIT, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB. |
<table>
<thead>
<tr>
<th>Product or solution</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOADPLUS</td>
<td>If you are unable to specify REGION=0M:</td>
</tr>
<tr>
<td></td>
<td>■ Specify NOLIMIT to allow unlimited above-the-bar memory.</td>
</tr>
<tr>
<td></td>
<td>■ If you are unable to specify NOLIMIT, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>Log Master</td>
<td>Specify at least 1 GB.</td>
</tr>
<tr>
<td>BMC Object Administration <em>for DB2</em></td>
<td>If you are unable to specify REGION=0M:</td>
</tr>
<tr>
<td></td>
<td>■ Specify NOLIMIT to allow unlimited above-the-bar memory.</td>
</tr>
<tr>
<td></td>
<td>■ If you are unable to specify NOLIMIT, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>BMC Performance <em>for DB2</em> Databases</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you are unable to specify REGION=0M:</td>
</tr>
<tr>
<td></td>
<td>■ Specify NOLIMIT to allow unlimited above-the-bar memory.</td>
</tr>
<tr>
<td></td>
<td>■ If you are unable to specify NOLIMIT:</td>
</tr>
<tr>
<td></td>
<td>— For DASD MANAGER, if above-the-bar memory limits are inadequate, contact your z/OS system administrator.</td>
</tr>
<tr>
<td></td>
<td>— For REORG PLUS, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>NGT Recover</td>
<td>Specify at least 2 GB, if you are operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>Recovery <em>for DB2</em></td>
<td>Specify at least 1 GB.</td>
</tr>
<tr>
<td>RECOVERY MANAGER</td>
<td>Specify at least 1 GB.</td>
</tr>
<tr>
<td>Recovery Management</td>
<td>Specify at least 2 GB, if you are operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>BMC Recovery <em>for DB2</em></td>
<td>Specify at least 2 GB, if you are operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>REORG PLUS</td>
<td>If you are unable to specify REGION=0M:</td>
</tr>
<tr>
<td></td>
<td>■ Specify NOLIMIT to allow unlimited above-the-bar memory.</td>
</tr>
<tr>
<td></td>
<td>■ If you are unable to specify NOLIMIT, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB.</td>
</tr>
<tr>
<td>Product or solution</td>
<td>Recommendation</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| UNLOAD PLUS        | If you are unable to specify REGION=0M:  
  ■ Specify NOLIMIT to allow unlimited above-the-bar memory.  
  ■ If you are unable to specify NOLIMIT, specify at least 4 GB; if you are operating on LOB or XML data, BMC recommends at least 32 GB. |

To override the default MEMLIMIT value

1. Use one of the following methods to override the default MEMLIMIT value:
   - Specify the MEMLIMIT parameter in the JCL.
   - Specify REGION=0M in the JCL.
   - Use the SMF IEFUSI exit.

Modifying installation options after customization

To modify the default values of installation options after customizing your product or solution, see “Modifying installation options modules” on page 146.  

*Note*  
For information about changing UIM server options, see “Changing UIM server options” on page 309.

Modifying installation options modules

If you modify any of the values in a $730DOPT job after customization, you must use the following procedure to apply the changes.

To apply changes to the $730DOPT job

1. After making the changes, rerun the $730DOPT job.

2. For products listed in the table Table 91 on page 147, if you changed the plan name, edit the bind job and bind the plan:
In the bind job listed for your product in Table 91 on page 147, change the plan name to the plan name in $730DOPT.

You must perform this action for each product for which you changed the plan name.

Change the product collection ID in the PKLIST statement (the first parameter of this statement) to match the plan name.

(Administrative products only) Edit the control table in the BMCDB2 CLIST by changing the name of the plan to match the plan name that you changed in $730DOPT. (For more information, see “Modifying the ISPF control table” on page 170.)

Rerun the bind job.

---

**Note**

If you are using data sharing and plan to use mixed versions of DB2 in the same data sharing group, complete the following steps:

1. Ensure that the DSNZPARM ABIND is set to COEXIST.

2. Use the earliest version of DB2 in the data sharing group to perform the bind.

Run the IVP job to verify that the changes took effect.

For more information, see “Verifying the Administrative products’ installation” on page 327 and “Verifying Backup and Recovery product and Utility product installation” on page 328.

**Table 91: Bind jobs**

<table>
<thead>
<tr>
<th>Product</th>
<th>Bind job</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALTER</td>
<td>ACM ssidB</td>
</tr>
<tr>
<td>BMCDSN</td>
<td>ABU ssidB</td>
</tr>
<tr>
<td>CATALOG MANAGER</td>
<td>ACT ssidB</td>
</tr>
<tr>
<td>CHANGE MANAGER</td>
<td>ACM ssidB</td>
</tr>
<tr>
<td>CHECK PLUS</td>
<td>ACK ssidB</td>
</tr>
<tr>
<td>DASD MANAGER PLUS</td>
<td>ASU ssidB</td>
</tr>
<tr>
<td>LOADPLUS</td>
<td>AMU ssidB</td>
</tr>
<tr>
<td>REORG PLUS</td>
<td>ARU ssidB</td>
</tr>
</tbody>
</table>
Increasing the size of DB2 active logs for LOADPLUS

For SQLAPPLY load jobs, LOADPLUS uses insert processing. Insert processing writes to your DB2 logs unless your table space is defined as NOT LOGGED. Therefore, if you are installing LOADPLUS, you might need to increase the size of your active logs.

For guidelines about sizing your active logs, see the IBM DB2 installation guide. For information about SQLAPPLY load jobs, see the LOADPLUS for DB2 Reference Manual.

Customizing products that prevent x37 abends in LOADPLUS

Products that prevent x37 abends must be customized to ensure that they work properly with EXCP processing in LOADPLUS.

When inadequate space is available for work data sets during job execution, the system issues an x37 abend and ends the job. Some sites use products such as the BMC MainView Storage Resource Manager (SRM) StopX37/II product to allocate additional volumes automatically when this condition occurs. However, those products might fail to intercept x37 abends if EXCP processing is in use.

LOADPLUS uses EXCP processing. Complete the following procedure to ensure proper handling of x37 abends.

To prevent x37 abends in LOADPLUS

1. Determine whether your site uses a product that intercepts x37 abends and whether that product is sensitive to EXCP processing.

See your DASD storage management system administrator for assistance.

<table>
<thead>
<tr>
<th>Product</th>
<th>Bind job</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNLOAD PLUS</td>
<td>ADU ssidB</td>
</tr>
</tbody>
</table>

a. The ssid variable represents the ID of the DB2 subsystem where you will run the job.
2 If you use MainView SRM StopX37, use one of the following methods to customize the product to prevent x37 abends in LOADPLUS.

**Note**

If you use a similar product from another vendor, see that product’s documentation regarding activating support for EXCP processing.

- Update the System Master Global member (the active SMMSYSxx member) in UBBPARM:
  
  ```
  SKIP=(PROG=AMUUMAIN,CHECK=(EXCP))
  ```

  Using this method eliminates the need to maintain the code in any subsequent RLST processing.

- Include the NOCHECK keyword in the specific SMRLSTxx member that is associated with the SPACVOLA function. (The variable `numberOfVolumes` represents the maximum number of volumes that can be available for volume extension.)
  
  ```
  SET SPACVOLA=numberOfVolumes NOCHECK=EXCP INC PGM=(AMUUMAIN)
  ```

  Using this method instructs the system to allow jobs that execute the listed programs to run regardless of whether those programs use EXCP processing.
Enabling interactions between products

You might need to complete additional steps to enable the products to interact with each other.

Enabling interaction between CATALOG MANAGER and BMC utilities (including Backup and Recovery products)

CATALOG MANAGER can interact with the BMCUTIL, BMCHIST, and BMCSYNC tables to provide BMC utility control, status, and history information.

Note
CATALOG MANAGER accesses the utility tables during batch processing and when using online commands.

Before you begin

Determine whether you need to perform this task and, if so, which parts of this task you need to perform:

- Perform this task if you installed CATALOG MANAGER in a separate installation session before you installed the utilities.
- Determine whether your current aliases point to the correct tables.
  CATALOG MANAGER uses the following aliases:
  - BMC_UTILITY for the BMCUTIL table
  - REORG_HISTORY for the BMCHIST table
— BMC_UTIL_SYNC and BMC_UTIL_SYNC2 for the BMCSYNC table

If the utilities are installed in a different load library than CATALOG MANAGER, use the task “To use the load library in which the utilities are installed” on page 152.

**To use the load library in which the utilities are installed**

1. In the HLQ.UBMCCNTL library, find the member that has the same name as the CATALOG MANAGER installation options module.

2. In the POFDS parameter of the member, note the name of the POF.

3. In the HLQ.UBMCCNTL library, find the POF member.

4. Update the following keywords with , (R) and update the POFDATE in the POF member to use the different utilities load libraries:
   - ADDLOAD1
   - ADDLOAD2
   - BMC_CHECK_LOAD
   - BMC_COPY_LOAD
   - BMC_LOAD_LOAD
   - BMC_RECOVER_LOAD
   - BMC_REORG_LOAD
   - BMC_UNLOAD_LOAD

5. If necessary, add any additional load libraries to SLIB member AJXSTEPU.

6. If you added load libraries in Step 5 on page 152, compile the SLIB member.

   For sample compile JCL, refer to member AJXCOMPS in the HLQ.BMCCNTL data set.

   **Note**

   If you want to modify the JCL in member AJXCOMPS, copy the member from HLQ.BMCCNTL to HLQ.UBMCCNTL. Then, modify the JCL in HLQ.BMCCNTL(AJXCOMPS).
Enabling interaction between ALTER or CHANGE MANAGER and BMC utilities (including Backup and Recovery products)

Use the following procedure to use a different utilities load library, if the utilities products are installed in a different load library than ALTER or CHANGE MANAGER.

Perform this task if you installed ALTER or CHANGE MANAGER under either of the following circumstances:

- You installed ALTER or CHANGE MANAGER in a separate installation session before you installed the utilities.
- You installed ALTER or CHANGE MANAGER either in the same installation session as the utilities or in a separate installation session after you installed the utility products, but you did not associate ALTER or CHANGE MANAGER with the utilities on the Product to Product Interface panel.

To use the load library in which the utilities are installed

1. In the \*HLQ.UBMCCNTL library, find the member that has the same name as the ALTER or CHANGE MANAGER installation options module.
2. In the POFDS parameter of the member, note the name of the POF.
3. In the \*HLQ.UBMCCNTL library, find the POF member.
4. In the POF member, update the following keywords with ,(R) and update POFDATE to use the different utilities load libraries:
   - ADDLOAD1
   - ADDLOAD2
   - BMC_CHECK_LOAD
   - BMC_COPY_LOAD
   - BMC_LOAD_LOAD
   - BMC_RECOVER_LOAD
   - BMC_REORG_LOAD
   - BMC_UNLOAD_LOAD
5. If necessary, add any additional load libraries to SLIB member AJXSTEPU.
6. If you added load libraries in Step 5 on page 153, compile the SLIB member.
For sample compile JCL, refer to member AJXCOMPS in the *HLQ.BMCCNTL* data set.

**Note**

If you want to modify the JCL in member AJXCOMPS, copy the member from *HLQ.BMCCNTL* to *HLQ.UBMCCNTL*. Then, modify the JCL in *HLQ.UBMCCNTL(AJXCOMPS)*.

---

## Enabling interaction between DASD MANAGER PLUS and BMC utilities (including Backup and Recovery products)

If you installed DASD MANAGER PLUS in a separate installation session before you installed the utilities, you must change the load library. To use DASD MANAGER PLUS with NGT Copy, you must direct the utility aliases to the correct DASD MANAGER PLUS tables and also direct the DASD MANAGER PLUS aliases to the appropriate utility tables.

### Before you begin

If you use the BMCSTATS runtime option, NGT Copy can update the DASD MANAGER PLUS statistics tables to update statistical information. The following table shows the aliases that the NGT Copy utility uses to reference the corresponding tables for DASD MANAGER PLUS.

### Table 92: DASD MANAGER PLUS table aliases for NGT Copy

<table>
<thead>
<tr>
<th>Alias</th>
<th>DASD MANAGER PLUS table a</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMCACP_BMCXTBSP</td>
<td>ATS(v_r).RS_TABLESPACE</td>
</tr>
<tr>
<td>BMCACP_BMCXTBPT</td>
<td>ATS(v_r).RS_TABLEPART</td>
</tr>
<tr>
<td>BMCACP_BMCXTBLS</td>
<td>ATS(v_r).RS_TABLES</td>
</tr>
</tbody>
</table>

1 The variable \(v_r\) represents the version and release number of your current DASD MANAGER PLUS product. These table names are the default names as shipped and might have changed when DASD MANAGER PLUS was installed.

### To direct the utility aliases to the DASD MANAGER PLUS tables

1. Drop the NGT Copy aliases.
2 Create the new NGT Copy aliases by using the same alias names, but use the correct DASD MANAGER PLUS table names.

**Note**

If DASD MANAGER PLUS tables are not connected or installed when you install NGT Copy, the associated package binds will complete with a return code 4.

**To use a different load library**

If the utilities are installed in a different load library than DASD MANAGER PLUS, use the following procedure to change the utilities load library.

1 In the *HLQ.UBMCCNTL* library, find the DASD MANAGER PLUS member that has the same name as the installation options module.

2 In the member, locate the name of the POF in the POFDS parameter.

3 In the *HLQ.UBMCCNTL* library, find the POF member.

4 Update the keywords with ,(R) and update the POFDATE in the POF member to use the different utilities load libraries:
   - ADDLOAD1
   - ADDLOAD2
   - BMC_COPY_LOAD
   - BMC_LOAD_LOAD
   - BMC_REORG_LOAD

5 If necessary, add any additional load libraries to SLIB member AJXSTEPU.

6 If you added load libraries in Step 5 on page 155, compile the SLIB member.

For sample compile JCL, refer to member AJXCOMPS in the *HLQ.BMCCNTL* data set.

**Note**

If you want to modify the JCL in member AJXCOMPS, copy the member from *HLQ.BMCCNTL* to *HLQ.UBMCCNTL*. Then, modify the JCL in *HLQ.UBMCCNTL(AJXCOMPS)*.
DASD MANAGER PLUS use within other products

You can use the DASD MANAGER PLUS product within ALTER, CHANGE MANAGER, and CATALOG MANAGER.

The Installation System automatically enables these products to interact with one another, if the following conditions exist:

- You are installing DASD MANAGER PLUS and ALTER, CHANGE MANAGER, or CATALOG MANAGER simultaneously

- You currently have DASD MANAGER PLUS installed and you are installing ALTER, CHANGE MANAGER, or CATALOG MANAGER

- You select to allow the products to interact with one another on the Install System Product to Product panel

However, if you install DASD MANAGER PLUS after you have installed ALTER, CHANGE MANAGER, or CATALOG MANAGER, you must perform additional procedures to use DASD MANAGER PLUS within these products.

**Note**

To enable the use of DASD MANAGER PLUS within ALTER, CHANGE MANAGER, or CATALOG MANAGER, you must select the runtime enablement feature when you install DASD MANAGER PLUS.

Enabling the use of DASD MANAGER PLUS within ALTER or CHANGE MANAGER

You can use DASD MANAGER PLUS within ALTER or CHANGE MANAGER.

The Installation System automatically enables this functionality if the following conditions exist:

- You are installing ALTER or CHANGE MANAGER and DASD MANAGER PLUS simultaneously.

- You currently have DASD MANAGER PLUS installed and you are installing ALTER or CHANGE MANAGER.
You select to allow the products to interact with one another on the Install System Product to Product panel.

To use DASD MANAGER PLUS within ALTER or CHANGE MANAGER

Complete this procedure if one of the following conditions exist:

■ You install DASD MANAGER PLUS after you install ALTER or CHANGE MANAGER, and the products do not share libraries.
■ You install DASD MANAGER PLUS into a separate library.

1 Edit the BMCDB2 CLIST:
   a Add the DASD MANAGER PLUS load library HLQ to the $HLQ2 variable.
   b Add the DASD MANAGER PLUS product information to the control table values in $HLQ2 CONTAB, as shown in Figure 1 on page 157.

Refer to the comments that precede the *DATA section of the control table for help with adding rows to the table.

Figure 1: Adding DASD MANAGER PLUS to the control table

<table>
<thead>
<tr>
<th>*DATA</th>
<th>PROD</th>
<th>SSID</th>
<th>D/</th>
<th>DOPT</th>
<th>PLAN</th>
<th>APPL</th>
<th>COLL_ID</th>
<th>NICKNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ASU</td>
<td>DBAP</td>
<td>D</td>
<td>ASUDOPD1</td>
<td>ASU930DC</td>
<td>ASUA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2 Update the ALTER or CHANGE MANAGER installation option for DASD MANAGER PLUS:
   a Set the DASDMAN option to (Y,R).
   b Reassemble the installation options module.

3 Edit the product options file (POF) and set the DASD_LOAD keyword to the DASD MANAGER PLUS load library or APF library. You must also update the keyword with ,(R) and update the POFDATE.
   a Set the DASD_LOAD keyword to the DASD MANAGER PLUS load library or APF library.
   b Update the keyword with ,(R).
   c Update the POFDATE.

4 Add the BMC Common Statistics collection list (ATS $vrn_D_MAIN.*) to the PACKLIST for the Front End, Specification, and Analysis plans.
5 Rebind the plans.

6 Copy the ASUVERSN member from the DASD MANAGER PLUS load library to the ALTER or CHANGE MANAGER load library.

Enabling the use of DASD MANAGER PLUS within CATALOG MANAGER

Within CATALOG MANAGER, you can use commands to invoke DASD MANAGER PLUS.

The following commands are valid:

- SPACE, which displays the Space Estimation panels for table spaces and indexes.
- STATS, which displays statistics panels for specified objects.

The Installation System automatically enables this functionality if the following conditions exist:

- You are installing CATALOG MANAGER and DASD MANAGER PLUS simultaneously, or
  - You currently have DASD MANAGER PLUS installed and you are installing CATALOG MANAGER.

- You select to allow the products to interact with one another on the Install System Product to Product panel.

To enable DASD MANAGER PLUS when one version exists

If one of the following conditions exists, perform the steps in the following procedure to use DASD MANAGER PLUS within CATALOG MANAGER:

- You install DASD MANAGER PLUS after you install CATALOG MANAGER and the products do not share libraries.
- You install DASD MANAGER PLUS into a separate library.

1 Edit the BMCDB2 CLIST.

   a Add the DASD MANAGER PLUS load library HLQ to the HLQ1 variable.

   b Add the DASD MANAGER PLUS product information to the control table values in HLQ.CONTAB, as shown in Figure 2 on page 159.
Refer to the comments that precede the *DATA section of the control table for help with adding rows to the table.

**Figure 2: Adding DASD MANAGER PLUS to the control table**

<table>
<thead>
<tr>
<th>*DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>*PROD</td>
</tr>
<tr>
<td>ASU</td>
</tr>
</tbody>
</table>

2 Update the CATALOG MANAGER installation option for DASD MANAGER PLUS:

   a Set the BOPTS option to ASUDOPD1 (or to the name of the DASD MANAGER PLUS installation options module).

   b Reassemble the installation options module.

3 Edit the product options file (POF) and set the DASD_LOAD keyword to the new DASD MANAGER PLUS load library or APF library.

**To enable DASD MANAGER PLUS when more than one version exists**

Depending on your environment and on the products and solutions that you have installed, you might have two versions of DASD MANAGER PLUS installed. If the following conditions exist, you must perform the steps in the following procedure to use DASD MANAGER PLUS within CATALOG MANAGER:

- You currently have CATALOG MANAGER and DASD MANAGER PLUS installed, and you are installing a new version of DASD MANAGER PLUS into a separate library.

- You want CATALOG MANAGER to interact with the new version of DASD MANAGER PLUS.

1 Back up all of the ASU* and ATS* load modules in your existing library (where * is a wildcard) into a backup data set.

2 Copy the ASU* and ATS* load modules from the new library and replace the existing ASU* and ATS* load modules in the old library.

3 Edit the BMCDB2 CLIST and add the new DASD MANAGER PLUS load library HLQ to the HLQ1 variable.

4 Update the CATALOG MANAGER installation options.

   a Set the BOPTS option to ASUDOPD1 (or to the name of the DASD MANAGER PLUS installation options module).

   b Reassemble the installation options module.
5 Edit the product options file (POF) and set the DASD_LOAD keyword to the new DASD MANAGER PLUS load library or APF library.

Enabling interaction between RECOVERY MANAGER and other products

You need to complete additional customization tasks to enable interaction between RECOVERY MANAGER and other products.

Enabling interaction between RECOVERY MANAGER and Log Master

To enable interaction between RECOVERY MANAGER and Log Master, Log Master must be installed and you must add some information to the RECOVERY MANAGER option set.

**To enable interaction between Log Master and RECOVERY MANAGER**

1 Add the Log Master load library name to the Log Master Load product option in the RECOVERY MANAGER option set.

Enabling interaction between RECOVERY MANAGER and NGT Recover

To enable interaction between RECOVERY MANAGER and NGT Recover, NGT Recover must be installed and you must add some information to the RECOVERY MANAGER option set.

**To enable interaction between NGT Recover and RECOVERY MANAGER**

1 Add the following information to the RECOVERY MANAGER option set:

<table>
<thead>
<tr>
<th>Product option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGT Recover Load</td>
<td>NGT Recover load library</td>
</tr>
</tbody>
</table>
Enabling interaction between NGT Copy and RECOVERY MANAGER

RECOVERY MANAGER can interact with NGT Copy.

When you install RECOVERY MANAGER and NGT Copy at the same time, this interaction is automatically enabled.

If you install the products at different times, you must ensure that they share the same common utilities (BMCUTIL) database so that NGT Copy can access object sets that are created by RECOVERY MANAGER.

Enabling interaction between RECOVERY MANAGER and PACLOG

To enable interaction between RECOVERY MANAGER and PACLOG, PACLOG must be installed and you must add some information to the PACLOG option set.

To enable interaction between RECOVERY MANAGER and PACLOG

1 Add the following information to the PACLOG option set:

<table>
<thead>
<tr>
<th>Product option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PACLOG Load</td>
<td>PACLOG load library</td>
</tr>
<tr>
<td>PACLOG CNTL</td>
<td>PACLOG CNTL library</td>
</tr>
</tbody>
</table>

Enabling the use of SQL Explorer for DB2 within CATALOG MANAGER

Within CATALOG MANAGER, you can use commands to invoke the SQL Explorer for DB2 production.

To invoke SQL Explorer, CATALOG MANAGER uses the ACTPSS CLIST. To enable the use of SQL Explorer within CATALOG MANAGER, you must customize the ACTPSS CLIST in the HLQ.UBMCCLIB data set. For more information about customizing the CLIST, see the Installation System documentation.
Customizing Administrative products

This chapter describes additional customization tasks that are specific for the administrative products.

Specific ALTER and CATALOG MANAGER customization tasks

In addition to the customization tasks for multiple products, you need to perform other customization tasks.

Creating indexes to improve performance

To improve performance, BMC recommends that you create indexes on the DB2 catalog tables.

To create indexes on the DB2 catalog tables

1. Follow the instructions in HLQ:UBMCCNTL(BMIDB2XA).

Note
When you are implementing catalog indirection, do not create indexes on copies of the DB2 catalog tables as the indexes already exist.

Shared components

The ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products share several components.
The following components are shared:

- JCL Generation, which controls the JCL generation process
- Execution Monitor, which controls worklist processing by reading and performing worklist commands
- Common SQL, which provides access to the DB2 catalog

When you unload ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS (or any solution that includes one or more of these products), these components are also unloaded. The Installation System copies these components to an APF-authorized load library that any of the products can share. If you install the products at different times or if you are applying maintenance and any of the products share the same APF-authorized load library, you must bind each product to the new level of the shared components.

**Note**
If you do not properly bind all of the products that share the common components, any attempts to generate JCL or to execute worklists can cause SQLCODEs -805 and -818. The product that has not been bound or upgraded will not run.

You do not have to bind a product separately to the shared components if the following conditions exist:

- You are using the same APF-authorized load library, and you are upgrading all products that use the shared components at the same time. The binds take place during the upgrade.
- You are using separate APF-authorized load libraries for your products.

**Note**
A problem occurs if all of the following conditions exist:

- You install one of the products or a solution that has one of the products as a component, and the product or solution uses the current version of the JCL Generation and Execution components.
- You install another product or solution that uses an earlier version of the JCL Generation and Execution components.

In this case, the products or solutions cannot use the same APF-authorized load library. To prevent the problem from occurring, choose a different load library when installing the additional product or solution.
Binding a product to shared components

Use the following procedure to bind ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS to the shared components.

To bind the products

1. Edit the BIND packages and plans for the product, which are in the HLQ.UBMCCNTL data set.

   The following table lists the member names for the jobs. The variable prd is the product or component code, and ssid is the DB2 subsystem ID.

<table>
<thead>
<tr>
<th>Member name</th>
<th>Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>prdssidP</td>
<td>Package BIND jobs for direct access</td>
</tr>
<tr>
<td>prdssidB</td>
<td>Plan BIND jobs (including CATALOG MANAGER plan BIND jobs for indirection)</td>
</tr>
<tr>
<td>prdssidZ</td>
<td>Package and plan BIND jobs for indirection (except CATALOG MANAGER plan BIND jobs)</td>
</tr>
</tbody>
</table>

2. Concatenate the new HLQ.BMCDBRM library ahead of the old HLQ.BMCDBRM library in the DBRMLIB DD statement in these members.

3. Submit the BIND jobs.

4. Repeat for each product and for the ACS component, if applicable.

Generating environment-specific JCL

You might need to change members of the BMC product skeleton library (SLIB) to generate environment-specific JCL. This procedure describes the steps you must perform to edit, test, and compile the SLIB. The JCL Generation component generates the JCL that is needed to execute all of the batch functions that use ISPF file tailoring.

To edit and compile SLIBs

1. Edit the appropriate SLIB members in HLQ.UBMCSLIB to change the way the JCL is generated.

   Note
   Any customizations that you have made to the SLIB members for an earlier release are not included in your current installation.
a  *(optional)* Edit the AJX#USRV member and change the EXEC REGION parameter.

The EXEC REGION parameter is set by default to REGION=0M in the AJX#USRV member that resides in the SLIB. If you do not change the IBM-supplied default limits in the IREALIMIT or IEFUSI exit routine modules, this parameter requests that the job step get all of the available storage above and below the 16 MB line.

b  Edit the AJX#DSNS member to generate JCL for GDGs.

2  Use JCL Generation to test the changes to the SLIB.

For more information about testing the SLIB members, refer to the following BMC books:

- *ALTER and CHANGE MANAGER for DB2 User Guide, Volume 2*
- *CATALOG MANAGER for DB2 User Guide*
- *DASD MANAGER PLUS for DB2 User Guide*

3  Compile the SLIB members that you edited.

For a sample compile JCL, refer to member AJXCOMPS in the *HLQ.BMCCNTL* data set. For more information about compiling the SLIB members, see the following BMC books:

- *ALTER and CHANGE MANAGER for DB2 User Guide, Volume 2*
- *CATALOG MANAGER for DB2 User Guide*
- *DASD MANAGER PLUS for DB2 User Guide*

**Note**

If you want to modify the JCL in member AJXCOMPS, copy the member from *HLQ.BMCCNTL* to *HLQ.UBMCCNTL*. Then, modify the JCL in *HLQ.UBMCCNTL(AJXCOMPS)*.

---

**Specifying generation data groups**

You can specify generation data groups (GDGs) by adding a symbolic variable to the local and recovery primary and backup copy keywords. As a result, the data set names are resolved using the symbolic variables, and include the GDG.
To specify a GDG

1. In the HLQ.UBMCCNTL library, find the member that has the same name as the product installation options module.

2. In the POFDS parameter of the member, note the name of the POF.

3. In the HLQ.UBMCCNTL library, find the POF member.

4. Add the symbolic (&GDG) to the end of the following keywords in the POF member:
   - PCPY1_PREFIX
   - PCPY2_PREFIX
   - RCPY1_PREFIX
   - RCPY2_PREFIX

Example

PCPY1='&PREFIX..&OBNOD..P&PART(&GDG)'

BMCDB2PR panel

The BMCDB2PR panel is part of the BMC-supplied ISPF interface that the Installation System generates.

This panel includes a product selection list from which you can select a product. It also includes a DB2 catalog access field, in which you can specify whether to use the DB2 catalog data directly or to use a copy or a view of the DB2 catalog (if applicable to the product or component).

You might need to add additional products to the selection list or modify the catalog access field after you install and customize ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS.

Adding products to the BMCDB2PR panel

The Installation System enables you to add products to the BMCDB2PR panel.

Before you begin

Determine the following information:

- Location of the BMCDB2PR panel
Location of the product’s CLIST

The three-character code for the product

The following table lists the BMC products that you can add to the BMCDB2PR panel.

Table 94: BMC products for BMCDB2PR panel

<table>
<thead>
<tr>
<th>Product</th>
<th>Product code</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPTUNE for DB2</td>
<td>ASQ</td>
</tr>
<tr>
<td>CHANGE ACCUMULATION PLUS</td>
<td>CAP</td>
</tr>
<tr>
<td>NGT Copy</td>
<td>ACP</td>
</tr>
<tr>
<td>EXTENDED BUFFER MANAGER for DB2</td>
<td>XBM</td>
</tr>
<tr>
<td>Log Master for DB2</td>
<td>ALP</td>
</tr>
<tr>
<td>OPERTUNE for DB2</td>
<td>DDT</td>
</tr>
<tr>
<td>PACLOG for DB2</td>
<td>ALM</td>
</tr>
<tr>
<td>RECOVERY MANAGER</td>
<td>ARM</td>
</tr>
</tbody>
</table>

Additional parameters, such as the SSID

To add the products

The UPDTBMC CLIST and the UPDTDB2 macro can be found in a customized installation library that the user creates while installing products from multiple tapes, or in the base installation library from a single product tape.

1 Copy the UPDTBMC CLIST from the HLQ.INSTALL library to a library in your SYSPROC concatenation.

2 Copy the UPDTDB2 macro from the HLQ.INSTALL library to a library in your SYSPROC concatenation.

3 To execute the CLIST, type TSO UPDTBMC on the COMMAND line.

4 In the Location of BMCDB2PR Panel? field, type the name of the library in which the panel resides.

5 In the Location of CLIST for Product Being Added? field, type the name of the library in which the CLIST resides.

6 In the Product Code for Product Being Added? field, type the three-character product code.
Modifying and validating the DB2 catalog access option on the BMCDB2PR panel

The BMCDB2PR panel might need slight customization before you run ALTER, CATALOG MANAGER, or CHANGE MANAGER with catalog indirection.

To modify and validate the option

1. Edit the BMCDB2PR panel in HLQ.UBMCPLIB.

2. Add `Indirect`, as follows:

   \[
   \text{+`DB2 Catalog Access`...} \,+(`Direct`, `Indirect`)\]

3. To validate the Indirect option, make the following changes:

   \[
   \text{ver (`catopt`, `nb`, `list`, `DIRECT`, `INDIRECT`, `D`, `I`) } -- \text{Uncomment this line}\n   \]

   \[
   \text{/*ver (`catopt`, `nb`, `list`, `DIRECT`, `D`) */} \quad \text{-- Comment out this line}\n   \]

4. Press `END` to exit.

Changing from ALTER to CHANGE MANAGER on the BMCDB2PR panel

Use the following procedure to modify the BMCDB2PR panel when you upgrade to CHANGE MANAGER from ALTER.

To change ALTER to CHANGE MANAGER

1. Edit the BMCDB2PR panel in HLQ.UBMCPLIB.

2. Change the product selection text.
   a. Find the following line:
      \[
      \text{+`Z%1 ALTER for DB2`} \quad \text{+`Change or migrate DB2 objects/structures`}\n      \]
   b. Replace the line with the following text:
      \[
      \text{+`Z%1 CHANGE MANAGER for DB2`} \quad \text{+`Manage changes to DB2 objects/structures`}\n      \]

3. Change the program name and product code.
   a. Find the following commands:
      \[
      \text{1.`CMD(`&BMCDB2M \quad +\n      \text{PGM(ALUFRONT) CFUNC(ALLOC) +\n      \text{&tvdebug ssid(&ssidnm) libdef(&lbdefflg) +\n      \text{shrappl(&shrappl) access(`catopt`) +}\n      \]

Chapter 5  Customizing Administrative products  169
b Change PGM(ALUFORNT) to PGM(ACMFRONT).

c Change PROD(ALU) to PROD(ACM).

4 Press **END** to exit.

---

**Control table**

By modifying the control table, you can add a product, specify the location of libraries, enable access to data sharing members, specify different libraries for SSIDs, and specify shared installation options.

*Note*

The data in the control table, which begins with the identifier *DATA, is placed in specific positions, and every data row must have an asterisk in column 73. Comment lines contain an asterisk (*) in column 1. The data in the control table is column specific.

---

**Modifying the ISPF control table**

Use the following procedure to modify the ISPF control table.

**To modify the control table**

1 Edit the control table in the *HLQ.CONTAB* data set.

2 Press END to exit.

3 If either of the following conditions exists, type **GENERATE** on the **COMMAND** line of the BMCDB2PR panel:

   - You edited your BMCDB2 CLIST to use a generated permanent ISPF table for the control table (specified **GENTABLE=Y** in the BMCDB2 CLIST)
   - You modified the control table that was previously generated

   This action rebuilds the ISPF control table in the *HLQ.UBMCTLIB* data set.
Adding a product to the control table

Use the following procedure to add a product to the control table.

To add a product to the control table

1. Edit the control table in the HLQ.CONTAB data set.

2. Add a line in the *PROD section for the product by using one of the following procedures:

   - If one product was installed into the same set of libraries as another product, add a line in the *PROD section for the product.
     The example in Figure 3 on page 171 shows the line that adds the CATALOG MANAGER product to the table. \( \text{vr} \) represents the version and release of the product.

   ```*DATA
   *PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME
   *----|----|-|--------|--------|----|------------------|------------------------
   ACT DBAP D ACTDOPD1 ACTvrDG ACTA
   ```

   - If one product was installed into a different set of libraries than another product, add a line in the *PROD section that specifies the high-level qualifier (HLQ) of the product libraries.
   In the example in Figure 4 on page 171, the line indicates the location of the CATALOG MANAGER libraries, which were installed into a different set of runtime libraries than DASD MANAGER PLUS.

   ```*DATA
   *PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME
   *----|----|-|--------|--------|----|------------------|------------------------
   ACT DBAP H HLQ_for_ACT
   ```

   In the example in Figure 5 on page 171, the lines indicate the location of the CATALOG MANAGER SMP/E libraries.

   ```*DATA
   *PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME
   *----|----|-|--------|--------|----|------------------|------------------------
   ACT DBAP T HLQ_for_DB
   ACT DBAP B HLQ_for_BB
   ACT DBAP X HLQ_for_XX
   ACT DBAP P HLQ_for_password
   ```
If the APF load library uses a different HLQ from other product libraries and is different from the variable APFLIB value in the control table, specify the line shown in Figure 6 on page 172 in the *PROD section.

**Note**

You cannot add an APF-authorized library to SMP/E libraries; you must be using runtime libraries to add an APF-authorized library.

---

**Figure 6: Specifying the location of the APF load library (runtime environment)**

<table>
<thead>
<tr>
<th>*DATA</th>
<th>*PROD</th>
<th>SSID</th>
<th>D/I</th>
<th>DOPT</th>
<th>PLAN</th>
<th>APPL</th>
<th>COLL_ID</th>
<th>NICKNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACT</td>
<td>DBAP</td>
<td>A</td>
<td>ADDTNL.APFL.LOAD</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 Press END to exit.

**Enabling access to data sharing members in the control table**

If you installed the DB2 products in a data sharing (sysplex) environment, you can enable access to all of the data sharing members or to the group attach name.

**To enable access**

1 Edit the control table in the HLQ.CONTAB data set.

2 Duplicate the table rows of the existing DB2 subsystem name for each member or group attach name.

3 Substitute the member or group attach name for the SSID column.

The example in Figure 7 on page 172 uses the group attach name GRP1. The VCAT control table variable is used by ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS to indicate the VSAM catalog alias that contains the data sets for the DB2 catalog (DBDBCAT).

---

**Figure 7: Enabling access to additional members**

<table>
<thead>
<tr>
<th>*DATA</th>
<th>*PROD</th>
<th>SSID</th>
<th>D/I</th>
<th>DOPT</th>
<th>PLAN</th>
<th>APPL</th>
<th>COLL_ID</th>
<th>NICKNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ASU</td>
<td>DBDB</td>
<td>D</td>
<td>ASUDOPD1</td>
<td>ASUvrDC</td>
<td>ASU7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACT</td>
<td>DBDB</td>
<td>D</td>
<td>ACTDOPD1</td>
<td>ACTvrDM</td>
<td>ACT8</td>
<td>ACTvr.D_MAIN</td>
<td>DBDB</td>
</tr>
<tr>
<td></td>
<td>ACM</td>
<td>DBDB</td>
<td>D</td>
<td>ACMDOPD1</td>
<td>ACMvrDF</td>
<td>ACMB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EXIT</td>
<td>DBDB</td>
<td>'SYS3.DBDB.DSNEXIT'</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LOAD</td>
<td>DBDB</td>
<td>'SYS2.DB2V1OM.DSNLOAD'</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HLQ</td>
<td>DBDB</td>
<td>BMCADMN.Vvrm.D10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VCAT</td>
<td>DBDB</td>
<td>DBDBCAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DDF</td>
<td>DBDB</td>
<td>DBDB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Specifying separate libraries in the control table

Use the following procedure to specify separate libraries in the control table.

To specify separate libraries

1. Edit the control table in the *HLQ.CONTAB* data set.

2. If your installation has more than one version of DB2, use separate libraries for each version.

Refer to the following scenarios as examples for editing the control table:

- **Scenario 1**: CATALOG MANAGER is installed on SSID DB10. The product libraries have an HLQ of BMC.DB10.*. Add the table shown in Figure 8 on page 173 to the control table.

Figure 8: Adding CATALOG MANAGER to subsystem DB10

```
/Data
*PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME
*----|----|-|--------|--------|----|------------------|-----------------------
ACT  DB10 D ACTDOPD1 ACTvrDG ACTA
*LIB  SSID Data Set Name
*----|----|-------------------------------|
EXIT DB10 'SYS3.DB10.DSNEXIT' *
LOAD DB10 'SYS2.DB2V10M.DSNLOAD' *
```

- **Scenario 2**: CATALOG MANAGER is installed on SSID DB11. The product libraries have an HLQ of BMC.DB11.*. Add the table shown in Figure 9 on page 173 to the control table.

Figure 9: Adding CATALOG MANAGER to subsystem DB11

```
/Data
*PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME
*----|----|-|--------|--------|----|------------------|-----------------------
ACT  DB11 D ACTDOPD1 ACTvrDG ACTA
*LIB  SSID Data Set Name
*----|----|-------------------------------|
EXIT DB11 'SYS3.DB11.DSNEXIT' *
LOAD DB11 'SYS2.DB2V11M.DSNLOAD' *
```
■ **Scenario 3**: In a runtime environment, if the BMCDB2 CLIST in *HLQ.JCL* is used to invoke CATALOG MANAGER for both SSIDs, add the lines in Figure 10 on page 174 to the control table.

**Figure 10: Running DB11 CATALOG MANAGER from the DB10 BMCDB2 CLIST (runtime environment)**

```
*DATA *
*PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME *
*----|--|--|--------|--------|----|------------------|------------------------*
ACT DB11 D ACTDOPD1 ACTvrDG ACTB             *
*LIB SSID Data Set Name *
*----|--|-------------------------------| ******
EXIT DB11 'SYS3.DB11.DSNEXIT'   *
LOAD DB11 'SYS2.DB2V11M.DSNLOAD' *
HLQ DB10 BMC.DB10  *
```

The HLQ in Figure 10 on page 174 instructs the BMCDB2 CLIST to use BMC.DB10 as the HLQ for products that are installed on SSID DB11. Figure 11 on page 174 shows the updated control table.

**Figure 11: Updated control table (runtime environment)**

```
*DATA *
*PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME *
*----|--|--|--------|--------|----|------------------|------------------------*
ACT DB10 D ACTDOPD1 ACTvrDG ACTA             *
ACT DB11 D ACTDOPD1 ACTvrDG ACTB             *
*LIB SSID Data Set Name *
*----|--|-------------------------------| ******
EXIT DB11 'SYS3.DB11.DSNEXIT'   *
LOAD DB10 'SYS2.DB2V10M.DSNLOAD' *
HLQ DB10 BMC.DB10  *
EXIT DB11 'SYS3.DB11.DSNEXIT'   *
LOAD DB11 'SYS2.DB2V11M.DSNLOAD' *
HLQ DB11 BMC.DB11  *
```

In an SMP/E environment, if the BMCDB2 CLIST in *HLQ.JCL* is used to invoke CATALOG MANAGER for both SSIDs, add the lines in Figure 12 on page 174 to the control table.

**Figure 12: Running DB11 CATALOG MANAGER from the DB10 BMCDB2 CLIST (SMP/E environment)**

```
*DATA *
*PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME *
*----|--|--|--------|--------|----|------------------|------------------------*
ACT DB10 D ACTDOPD1 ACTvrDG ACTB             *
*LIB SSID Data Set Name *
*----|--|-------------------------------| ******
EXIT DB11 'SYS3.DB11.DSNEXIT'   *
LOAD DB11 'SYS2.DB2V11M.DSNLOAD' *
DB DB10 BMC.DB10.DBHLQ  *
BB DB10 BMC.DB10.BBHLQ  *
XX DB10 BMC.DB10.XXHLQ  *
PSWD DB10 BMC.DB10.PSWDHLQ *
```

Figure 13 on page 174 shows the updated control table.

**Figure 13: Updated control table (SMP/E environment)**

```
*DATA *
*PROD SSID D/I DOPT PLAN APPL COLL_ID NICKNAME *
*----|--|--|--------|--------|----|------------------|------------------------*
ACT DB10 D ACTDOPD1 ACTvrDG ACTB             *
*LIB SSID Data Set Name *
*----|--|-------------------------------| ******
EXIT DB11 'SYS3.DB11.DSNEXIT'   *
LOAD DB11 'SYS2.DB2V11M.DSNLOAD' *
DB DB10 BMC.DB10.DBHLQ  *
BB DB10 BMC.DB10.BBHLQ  *
XX DB10 BMC.DB10.XXHLQ  *
PSWD DB10 BMC.DB10.PSWDHLQ *
```
3 Press END to exit.

**Specifying the same installation options module in the control table**

You can specify the same installation options module for ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS to be shared between two or more DB2 subsystems.

**Before you begin**

ALTER, CHANGE MANAGER, CATALOG MANAGER or DASD MANAGER PLUS must be at the same version and release level on each of the DB2 subsystems. In addition, for ALTER or CHANGE MANAGER, the DB2 subsystems must be at the same version and release level.

The DB2 exit and load data sets, if different for each DB2 subsystem, must be removed from the installation options modules and put into a LINKLIST concatenation for use by foreground and batch processes.

**To specify the same installation options module**

1 For each of the products, choose one installation options module to represent the product’s installation options for all relevant DB2 subsystems.

2 Verify that the control table contains distinct and correct values for the VCAT variable.

3 Change the control table installation options values specified for the product and SSID to the shared installation options module name.
Application IDs in the control table

The control table allocates the ISPF application ID based on DB2 subsystem access.

During installation, the Installation System attempts to make each ISPF application ID unique across DB2 subsystems.

By default, the first time that the Installation System generates the control table, individual application IDs prdA are specified, where prd is the three-character product code. The shared application ID ADMA is also specified.

If you use the SSID installation method to perform a second or subsequent installation, the Installation System attempts to scan the existing control table and to allocate a unique application ID. For example, if CATALOG MANAGER is initially installed on DB2T, the application ID is ACTA. If CATALOG MANAGER is installed on DB2P, the Installation System scans the BMCDB2 CLIST and uses application ID ACTB because ACTA is already in use. The shared application ID for an SSID installation is ADMB.

When you access ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS, you can specify to use a shared or individual application ID, and the control table establishes the ISPF application ID and allocates the installation options module name. The product that receives control either initializes or refreshes your options with the information from the installation options module and the POF that is allocated by the control table.

Application IDs for multiple SSIDs

In some situations, when you make changes in one environment, those changes appear in another environment.

This situation usually happens when the same ISPF application ID is being established for multiple SSIDs, and is probably unacceptable because the user-option changes are SSID specific.

For example, if both of the DB2T and DB2P individual application IDs for CATALOG MANAGER are established as ACTA, any changes to user options that are made for DB2T are also made for the DB2P user options. The same is true for a shared application ID of ADMA used by DB2T and DB2P.

To avoid accidentally overlaying user options, ensure that the ISPF application that is established for each DB2 SSID is unique. The Installation System attempts to make each application ID unique in a given control table. It does not, however, make each application ID unique across multiple control tables. For example, if you execute the installation for DB2T and for DB2P, you have two control tables—one for each environment. The initial ISPF application ID for both SSIDs is xxxA, which results in an overlay.
If you are planning to execute multiple copies of the BMCDB2 CLIST and control table, change the ISPF application ID that the control table allocates so that each SSID user profile is unique across all control tables (see Figure 14 on page 177).

**Note**

If you do not change the application IDs, changing user options in one SSID might also change the same user options for a different SSID.

### Figure 14: Sample control table (runtime environment)

<table>
<thead>
<tr>
<th>*DATA</th>
<th>*PROD</th>
<th>SSID</th>
<th>D/I</th>
<th>DOPT</th>
<th>PLAN</th>
<th>APPL</th>
<th>COLL_ID</th>
<th>NICKNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXIT</td>
<td>xxxx</td>
<td>‘DB2.DSNEXIT’</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOAD</td>
<td>xxxx</td>
<td>‘DB2.DSNLOAD’</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HLQ</td>
<td>xxxx</td>
<td>BMCADMN.Vvrm.D81</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VCAT</td>
<td>xxxx</td>
<td>xxxx CAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDF</td>
<td>xxxx</td>
<td>xxxx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APPL</td>
<td>xxxx</td>
<td>ADMA#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the sample shown in Figure 14 on page 177, the variable xxxx is the SSID name and # is a unique one-byte character (such as A for the first SSID, B for the second SSID, C for the third, and so on).

### Subsequent DB2 subsystems in the control table

The Installation System generates member BMCDB2SS to support subsequent DB2 subsystems.

This member contains logic for the installation options module allocation. When you use this member to update the control table, consider the following points:

- If you have MVS/ESA and TSO/E version 2.1 or later, the Installation System prompts you for the location of the control table and automatically updates it with the information in the BMCDB2SS.
- If you do not have MVS/ESA and TSO/E version 2.1 or later, follow the directions in BMCDB2SS for updating the control table.
- If you are installing CATALOG MANAGER, follow the instructions for modifying the CATALOG MANAGER plan name.
Catalog indirection in the control table

Member BMCDB2CI is generated to support catalog indirection for ALTER, CATALOG MANAGER, or CHANGE MANAGER.

This member contains logic for the installation options module allocation for indirect access. When you use BMCDB2CI to update the control table, consider the following points:

- If you have MVS/ESA and TSO/E 2.1 or later, the Installation System automatically updates the control table with BMCDB2CI. The Installation System searches both the JCL output file and the installation file to apply the updates wherever a copy of the control table is found. The Installation System prompts you for the location of the control table.

- If you do not have MVS/ESA and TSO/E 2.1 or later, follow the directions in BMCDB2CI for updating the control table.

- If you are installing CATALOG MANAGER, follow the instructions for modifying the CATALOG MANAGER plan name.

Fast Path Navigation

For ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS, the Installation System provides Fast Path Navigation, which enables you to switch from one product to another without leaving the current product.

To initiate Fast Path Navigation, on the COMMAND line of the current product, enter the name of the product to which you want to switch. The following table provides a list of the products and commands.

<table>
<thead>
<tr>
<th>Product</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALTER</td>
<td>BMCALTER</td>
</tr>
<tr>
<td>CATALOG MANAGER</td>
<td>BMCCAT</td>
</tr>
<tr>
<td>CHANGE MANAGER</td>
<td>BMCCCHG</td>
</tr>
<tr>
<td>DASD MANAGER PLUS</td>
<td>BMCDASD</td>
</tr>
</tbody>
</table>

For example, if you are currently using DASD MANAGER PLUS and want to view an object description in CATALOG MANAGER, enter BMCCAT on the DASD MANAGER PLUS COMMAND line. When you initiate Fast Path Navigation, the
main menu for the requested product is displayed. In this case, the DASD MANAGER PLUS session is temporarily suspended and then resumed when you exit CATALOG MANAGER.

To use Fast Path Navigation, the following conditions must be met:

- You must install the products by using the Installation System.
- You must use the BMCDB2 CLIST during product invocation.
- The distributed CLISTs AEXADMF1 and AEXADMF2 must be in a data set that is either in the ALTLIB list of the BMCDB2 CLIST or in your SYSPROC concatenation.
- The product to which you are switching must be installed and reside in the same set of libraries as the product from which you are switching.
- For CATALOG MANAGER, you must enable the ELO (Editor Lock Options) command in the AEXADMF1 and AEXADMF2 CLISTs.

**Note**
You cannot use Fast Path Navigation to access a product that is currently suspended. For example, if you switch from ALTER to DASD MANAGER PLUS, you cannot use Fast Path to return to ALTER because it is currently suspended. Instead, you have to exit the DASD MANAGER PLUS session to resume the ALTER session.

---

### Specifying minimum TSO region size

ALTER, CHANGE MANAGER, DASD MANAGER PLUS, BMC Workbench, and CATALOG MANAGER require that you configure a TSO region size of 32 MB or greater for each user who signs on.

### Modifying POF values

Modifying your POF values does not require reassembly or linkage.

This procedure is available only for ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS.

1. Locate the POF in the `HLQ.BMCCNTL` data set, make any required changes, and save the changes.
Some of the options in the JCL Generation POF provide values for your ISPF user options. You can use the refresh capability to update these values. For more information, see “Modifying user profile values” on page 180.

Modifying user profile values

You can modify the values in the installation options module or in the POF for a product on an individual basis by using the product’s user options. These user options are saved and maintained in the user profile.

This is available only for ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS.

If you need to reset the values in the user profiles, you can use a refresh feature. This feature modifies one or more option values for all of the product’s users.

Refreshing installation options values in the user profile

To refresh an option value in all existing user profiles, enclose the option value in parentheses and include ,R after the value inside the parentheses.

The following example illustrates how to refresh the option value:

```
SSID=(DB2J,R),
```

**Note**

Do not drop either the continuation comma after the closing parenthesis or the continuation character in column 72.

This example refreshes the default DB2 subsystem ID for all users of the product.

For products other than CATALOG MANAGER, the ,R in the variable syntax indicates that the value specified will refresh the existing value of the variable in the user’s ISPF profile data set, if the time stamp of the installation options module is later than that in the user’s ISPF profile member. However, the user can change the override value in the user profile. In CATALOG MANAGER, the refresh occurs every time that a user starts the product.

To troubleshoot refreshing installation options values

1. Verify that the refresh option is coded on the correct macro listing keyword in the installation options assembly member.
2 Verify that the installation options assembly was completed successfully with a return code of 0.

If you receive assembly errors, compare your installation options module listing with one that the installation process generated. Some common errors are as follows:

- Missing comma delimiter after keyword value
- Missing continuation character in column 72
- Incorrect symbol-variable substitution
- Missing or unbalanced single quotation marks

3 Verify that the assembled installation options member is the same installation options member that ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS use.

   a To verify, access the environment information for your product as follows:

      ■ In ALTER or CHANGE MANAGER, on the main menu, type `ENVI` on the `COMMAND` line.
      ■ In CATALOG MANAGER, on the Primary Menu panel or any list panel, type `ENVI` on the `COMMAND` line.
      ■ In DASD MANAGER PLUS, on the main menu, select `User Options`. Then select `Current environment information`.

   b Compare the listed installation options module name with the name of the installation options module that you assembled and link-edited.

4 Verify that the installation options module assembly is updating the correct load library.

   The `SYSLMOD ddname` statement should refer to the load library where the products reside.

Refresh POF values in the user profile

You can specify a value to refresh the existing value of the variable in the user’s ISPF profile data set.
To refresh an option value

1. To refresh an option value, modify the value of the POF keyword in one of the following ways:

   - Include ",(R) after the option value, as in the following example:
     
     ```
     BMC_LOAD_OPTS=AMU$MMS,(R)
     ```

   - Specify a blank and ",(R), as in the following example:
     
     ```
     BMC_LOAD_OPTS= ,(R)
     ```

   These examples refresh the name of the LOADPLUS user options module.

   **Note**
   
   If the value for the POF keyword ends with a comma, as in the following example, include ",(R) after the comma.
   
   ```
   JOBCARD1=//JOBC JOB(&ZACCTNUM),’&PGMR’,,(R)
   ```

   When the POFDATE parameter is later than the previous POFDATE that is stored in the user’s ISPF profile, the specified value refreshes the existing value of the variable in the user’s ISPF profile data set.

To troubleshoot refreshing POF values

1. Verify that the refresh option is coded on the correct POF keyword.

2. Verify the date in the POFDATE parameter.

Using catalog indirection with ALTER, CATALOG MANAGER, and CHANGE MANAGER

After you install and customize your products, you can implement catalog indirection for ALTER, CATALOG MANAGER, or CHANGE MANAGER.

Catalog indirection is an optional method of implementing and maintaining these products. To accomplish catalog indirection, the products use aliases that point to a copy of the DB2 catalog.

Catalog indirection allows products to query the DB2 catalog indirectly. Catalog indirection applies only to catalog queries. Any action that changes information in the catalog must operate on the actual catalog, not on a copy of the catalog. For example, when you issue a command through CATALOG MANAGER to update the catalog, the action affects the actual catalog, the Execution Monitor in ALTER and CHANGE MANAGER also executes a worklist against the actual catalog.
contrast, the Analysis component in ALTER and CHANGE MANAGER can use either the actual catalog or catalog indirection when creating worklists.

General points about catalog indirection are as follows:

- Catalog indirection requires DB2 Version 10 or later in new-function mode.
- The products are set up to access the DB2 catalog directly. After the installation, you can use the Installation System to implement and maintain catalog indirection.
- The aliases that reference the DB2 catalog are hardcoded in the components. You direct the aliases to the catalog, copy, or views during installation by providing information on the Installation System panels.
- You can use the same copy or view of the catalog for CATALOG MANAGER and CHANGE MANAGER, or you can implement catalog indirection through separate copies for each product.
- Catalog indirection reduces contention for the DB2 catalog

To install catalog indirection, see the Installation System documentation.

**Implement and maintain catalog indirection**

Successful implementation of catalog indirection requires an in-depth understanding of the DB2 environment and its catalog structure, and experience in maintaining DB2 applications.

Each method of implementing catalog indirection should be managed as if catalog indirection were a DB2 application. Test the products fully without catalog indirection before you implement catalog indirection.

- Implement catalog indirection
  You can install catalog indirection for one or more of the products on one DB2 subsystem at a time. When you implement catalog indirection, the products use the existing product libraries and support the use of your own VSAM data sets. Optionally, the products can create a copy of the DB2 catalog by using the CREATE LIKE DDL syntax and create views of the DB2 catalog.

- Maintain catalog indirection
  You can apply maintenance to catalog indirection on one or more products on one DB2 subsystem at a time. You should perform maintenance if you have an existing copy of the DB2 catalog and have performed a new installation of the products.
Specify the installation options module

When a product runs, it uses its own installation options module that was built during installation. The BMCDB2 CLIST allocates the installation options module when you start the product.

When accessing the DB2 catalog with catalog indirection, the BMCDB2 CLIST allocates an indirect installation options module. This indirect installation options module must have a different name than the direct installation options module that was previously built.

The installation options module, the plan and collection IDs, and the alias qualifier are all crucial for the implementation of catalog indirection. The qualifier of the plan and the packages is used to resolve aliases that point to a copy of the DB2 catalog, depending on the method of implementation. You should understand their use and interaction before you implement catalog indirection.

The installation options module uses the convention prdDOPyz. Table 96 on page 184 describes the variables for the installation options module.

Table 96: Installation options module variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>prd</td>
<td>Product code</td>
</tr>
<tr>
<td>y</td>
<td>Access type (D=direct, I=indirect)</td>
</tr>
<tr>
<td>z</td>
<td>SSID indicator</td>
</tr>
</tbody>
</table>

Table 97 on page 184 shows examples of installation options modules.

Table 97: Examples of installation options modules

<table>
<thead>
<tr>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACMDOPDT</td>
<td>ALTER direct access for a test DB2 subsystem</td>
</tr>
<tr>
<td>ACMDOPIT</td>
<td>ALTER indirect access for a test DB2 subsystem</td>
</tr>
</tbody>
</table>

Unlike ALTER and CHANGE MANAGER, CATALOG MANAGER is designed to use a single installation options module for both direct and indirect access. The BMCDB2 CLIST allocates the same installation options module and thus the same plan for direct access and indirect access. The plan that is accessed contains two distinct collection IDs that are used to access direct or indirect catalogs. To implement a single installation options module, the installation dialog panels must process the CATALOG MANAGER installation options module differently from the installation options module of ALTER and CHANGE MANAGER.
The processing differences for CATALOG MANAGER are that during installation of catalog indirection, you are prompted for the creator of the CATALOG MANAGER indirect aliases, for the indirect collection ID, and for the name of the direct options module. All other installation options module information has been previously gathered.

**Note**

Do not regenerate the catalog indirect JCL for CATALOG MANAGER and then resume installation at a step *later* than the step that assembles the installation options module; doing so would cause the BINDs for the packages to fail because the value of the indirect collection ID would be unresolved. You must run the installation options module assembly step to resolve this value.

---

**Specify alias qualifiers during maintenance**

If you are applying maintenance to catalog indirection, you must specify the alias qualifier that is currently the owner of the products’ aliases. This qualifier must be the qualifier that you supplied when you originally installed catalog indirection for the products.

Maintenance for catalog indirection does not create any new DB2 objects, but it does re-create the existing aliases.

The Installation System uses one of the following three- or four-character prefixes when creating the aliases for ALTER and CHANGE MANAGER. Table 98 on page 185 describes the prefixes.

**Table 98: Alias prefixes**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT</td>
<td>Used by the Specification component of ALTER and CHANGE MANAGER The aliases are also used by the JCL Generation component’s data set sizing function.</td>
</tr>
<tr>
<td>CAT2</td>
<td>Used by the Analysis component of ALTER and CHANGE MANAGER, and the CM/PILOT component of CHANGE MANAGER <strong>WARNING:</strong> CAT2 aliases should not be redirected if the copy of the catalog has not been refreshed to match the DB2 catalog.</td>
</tr>
<tr>
<td>CAT3</td>
<td>Used by the Import component of ALTER and CHANGE MANAGER, and the Baseline and Compare components of CHANGE MANAGER <strong>WARNING:</strong> CAT3 aliases should not be redirected.</td>
</tr>
</tbody>
</table>
The Execution component always accesses the DB2 catalog directly and does not use aliases.

**Use a copy of the catalog**

Maintaining a copy of the catalog uses additional DASD space. The amount of space that is required equals the size of your DB2 catalog and can vary greatly, depending on your DB2 system.

You need to update the copy of the catalog on a timely basis to keep it accurate. Running the copy job does not have a significant impact on catalog contention but does consume other system resources. How often you should run the job depends on the amount of catalog change activity in your DB2 system and the type of users who are restricted to accessing a copy. A high-activity data center might need to run the job several times a day.

In addition, the job that updates the catalog copy prevents users from accessing the current copy of the catalog while the job runs. This restriction might have a negative impact on the products if you must run the copy job during a high-activity period.

**Note**
The SEARCH command in CATALOG MANAGER uses dynamic structured query language (SQL). To enable the SEARCH command to work on the copy of the catalog that catalog indirection uses, either run GRANT SELECT ON TABLE statements or bind with Dynamic Rules (BIND) on the main plan.

**Use a copy of the catalog to reduce catalog contention**

Contention for the DB2 catalog can be a problem for data centers that have high DB2 transaction rates. Because the products require frequent access to the DB2 catalog, they can contribute to catalog contention.

To improve performance by reducing catalog contention, you can perform the following actions:

- Tune the copy of the catalog.
- Add your own indexes to the copy of the catalog.
- Reorganize the tables or table spaces of the copy of the catalog.
- Direct the information queries from specific groups of users to a recent copy of the DB2 catalog. The components also perform better because they do not have to compete with other applications for DB2 catalog information.

For catalog indirection to be effective, you must ensure that the copy of the catalog reflects the status of the actual catalog. The degree of accuracy that is required depends on the types of users who are involved and the purpose of their information queries. The job that updates the catalog copy temporarily halts all information queries made through the copy.

### Specific CATALOG MANAGER customization tasks

In addition to the customization tasks for multiple components and for ALTER and CATALOG MANAGER, you need to perform customization tasks for CATALOG MANAGER.

### Access to catalog information

CATALOG MANAGER uses dynamic SQL to access DB2 catalog tables or product log tables.

CATALOG MANAGER observes the privileges of the user who lists the tables.

CATALOG MANAGER does not bypass any DB2 security when it generates and executes SQL, DML, or DB2 commands. DB2 rejects any action requested by CATALOG MANAGER for which the user is not authorized by DB2.

DB2 requires that users have at least the SELECT privilege to access catalog tables or product log tables. The CATALOG MANAGER installation options settings cannot override the DB2 SELECT authorization requirement.

### Prohibiting access to CATALOG MANAGER functions

The CATALOG MANAGER initial command restricts users from all CATALOG MANAGER functions except data editing.

When the initial command is enabled, CATALOG MANAGER starts at the Edit DB2 Table Options panel where users can set options for editing data, controlling the display of data, and processing SQL. Users can navigate through all data editing
panels, but cannot access the Primary Menu panel or other function panels. When users press END from the Edit DB2 Table Options panel, CATALOG MANAGER closes.

**WARNING**

You cannot enable both the initial command and the entry panel command (see “Specifying an entry panel” on page 188) in the same BMCDB2 CLIST.

---

**To enable the initial command**

1. Edit the BMCDB2 CLIST.

2. Find the lines that are shown in Figure 15 on page 188.

```bash
WHEN(ACTEMAIN) DO /* CATALOG MANAGER */
  SET BMCFPCNT= 10100
  IF (&ACCESS = INDIRECT) THEN +
  SET CIACCESS = YES
  SET APPLID = &ACTAPPL
  SET PARM = &STR(S=&SSID,O=&ACTDOPT,D=&ASUDOPTD,+M=BC,I=&CIACCESS,A=&ACMDOPT,+DB2CAT=&DB2VCAT )
/* EDITOR LOCK OPTIONS (ELO) - ALLOWS USER TO IDENTIFY */
/* THE DEFAULT LOCKING OPTIONS FOR DATA EDITING. USER */
/* MAY CHOOSE ALL OR ANY COMBINATION OF THE THREE. */
/* T - TABLE LOCK, R - ROW LOCK, N - NO LOCKING */
  SET PARM = &STR(&PARM,ELO=TRN)
/* UNCOMMENT 'SET PARM' LINE BELOW TO ALLOW ACCESS ONLY */
/* TO DATA EDITING FUNCTION. USERS CANNOT ACCESS OTHER */
/* CATALOG MANAGER FUNCTIONS. */
/* *-------------------------------------------------------------------------*/
  SET PARM = &STR(&PARM,E=EDIT) */
/* *-------------------------------------------------------------------------*/
```

3. As directed in the CLIST, uncomment the following line:

```bash
/* SET PARM = &STR(&PARM,E=EDIT) */
```

4. Press END to exit.

---

**Specifying an entry panel**

You can optionally cause CATALOG MANAGER to display an entry panel other than the Primary Menu panel by adding an entry panel command to the BMCDB2 CLIST.

The entry panel command is a CATALOG MANAGER single command of 1 through 48 characters that is passed as a parameter to the CATALOG MANAGER product module ACTEMAIN from the BMCDB2 CLIST. Users have access to all functions of
CATALOG MANAGER unless they have been restricted by other means, such as a customized session profile.

---

**WARNING**

You cannot enable both the entry panel command and the initial command in the same BMCDB2 CLIST.

---

**To edit the BMCDB2 CLIST to enable a different entry panel**

1. Edit the BMCDB2 CLIST.

2. Find the lines that are shown in Figure 16 on page 189.

   **Figure 16: BMCDB2 CLIST—CATALOG MANAGER entry panel**

   ```
   WHEN(ACTEMAIN) DO /* CATALOG MANAGER
   SET BMCFPCNT= 10100
   IF (&ACCESS = INDIRECT) THEN +
   SET CIACCESS = YES
   SET APPLID  = &ACTAPPL
   SET PARM    = &STR(S=&SSID,O=&ACTDOPT,D=&ASUDOPTD,+ +
   M=BC,1=&CIACCESS,A=&ACMDOPT,+ +
   DB2CAT=&DB2VCAT )
   /* EDITOR LOCK OPTIONS (ELO) - ALLOWS USER TO IDENTIFY */
   /* THE DEFAULT LOCKING OPTIONS FOR DATA EDITING, USER */
   /* MAY CHOOSE ALL OR ANY COMBINATION OF THE THREE. */
   /* T - TABLE LOCK, R - ROW LOCK, N - NO LOCKING */
   SET PARM = &STR(&PARM,ELO=TRN)
   /* UNCOMMENT 'SET PARM' LINE BELOW TO ALLOW ACCESS ONLY */
   /* TO DATA EDITING FUNCTION. USERS CANNOT ACCESS OTHER */
   /* CATALOG MANAGER FUNCTIONS. */
   /*---------------------------------------------------------------------------*/
   /*  SET PARM = &STR(&PARM, E=EDIT) */
   /*---------------------------------------------------------------------------*/
   3. Replace the command E=EDIT with the entry panel command. The entry panel command syntax is C=command.

   **Note**

   If the CATALOG MANAGER command that you specify requires a function or object type and qualifier, you must include them when defining the entry panel command parameter.

4. Uncomment the line that includes the entry panel command.

   The following example shows the edited line from the BMCDB2 CLIST to specify the CONNECT entry panel command.

   ```
   SET PARM = &STR(&PARM,C=CONNECT)
   ```

5. Press **END** to exit.
Specifying locking options for editing data

CATALOG MANAGER offers three locking options for editing table data: shared table lock, row lock, and no lock.

To set the editor locking options for all users, you must enable the locking options command. The command is passed as a parameter to the CATALOG MANAGER product module ACTEMAIN from the BMCDB2 CLIST.

To enable the locking options command

1. Edit the BMCDB2 CLIST.
2. Find the lines shown in Figure 17 on page 190.

```
WHEN(ACTEMAIN) DO /* CATALOG MANAGER
  SET BMCFPCNT= 10100
  IF (&ACCESS = INDIRECT) THEN +
  SET CIACCESS = YES
  SET APPLID  = &ACTAPPL
  SET PARM    = &STR(S=&SSID,O=&ACTDOPT,D=&ASUDOPTD,+
        M=BC,I=&CIACCESS,A=&ACMDOPT,+
        DB2CAT=&DB2VCAT)
  /* EDITOR LOCK OPTIONS (ELO) - ALLOWS USER TO IDENTIFY                       */
  /* THE DEFAULT LOCKING OPTIONS FOR DATA EDITING. USER                        */
  /* MAY CHOOSE ALL OR ANY COMBINATION OF THE THREE.                           */
  /* T - TABLE LOCK, R - ROW LOCK, N - NO LOCKING                              */
  SET PARM = &STR(&PARM, ELO=TRN)
```

3. Enable the CATALOG MANAGER locking options command.

   The syntax for the locking options command is `ELO=option`.

   As an example, Figure 17 on page 190 shows the locking option command ELO set to TRN. These options determine whether requests for edits from any user are allowed while a table is edited. For more information about the options for data editing, see the CATALOG MANAGER for DB2 User Guide.

4. Press END to exit.

   **Note**

   The CATALOG MANAGER data editing package ACTJTEQ is installed with the following values for two BIND PACKAGE options: an ISOLATION value of CS (cursor stability) and a CURRENTDATA value of YES. You can change these values by rebinding the data editing package with other values that are allowed by DB2. For BIND PACKAGE syntax and descriptions, see the IBM documentation.

5. If you plan to use Fast Path Navigation (see “Fast Path Navigation” on page 178), you must edit the AEXADMF1 and AEXADMF2 CLISTs and enable the
CATALOG MANAGER locking options command as you did in Step 3 on page 190 for the BMCDB2 CLIST.

For example, if you set ELO to TRN, then add the following statement to the AEXADMF2 CLIST:

```
SET PARM = &STR(&PARM,ELO=TRN)
```

Setting the session profile

The CATALOG MANAGER session profile enables you to customize specific product displays and operations for specific users or groups of users.

To initially set the session profile for all user groups, you must invoke the session profile command. The CATALOG MANAGER session profile command (1 to 18 characters) that calls a set of user-customized features that is saved under a specific session profile name. The session profile command is passed as a parameter to the CATALOG MANAGER product module ACTEMAIN from the BMCDB2 CLIST.

To invoke the session profile command

1. Edit the BMCDB2 CLIST.

2. Find the lines that are shown in Figure 18 on page 191.

```
/*----------------------------------------------------------*/
/* EDITOR LOCK OPTIONS (ELO) - ALLOWS USER TO IDENTIFY THE */
/* DEFAULT LOCKING OPTIONS FOR DATA EDITING. USER MAY CHOOSE */
/* ALL OR ANY COMBINATION OF THE THREE. T - TABLE LOCK, */
/* R - ROW LOCK, N - NO LOCKING. */
/*----------------------------------------------------------*/
SET PARM = &STR(&PARM,ELO=TRN)
```

3. Add the following command after the ELO locking option command:

```
SET PARM = &STR(&PARM,PR=profileName)
```

**Example**

Adding the following line in the CLIST causes CATALOG MANAGER to invoke the session profile that is named PROGRAMMERS:

```
SET PARM = &STR(&PARM,PR=PROGRAMMERS)
```

4. Press END to exit.
Editing the CONNECT command servers

The servers that the CATALOG MANAGER product uses in the CONNECT command are listed in the control table.

To edit the control table to change or enable the servers

1. Edit the control table.

2. To change the servers that are listed for the CONNECT command (see Figure 19 on page 192), you can add, delete, or modify the data rows.

Figure 19: CATALOG MANAGER CONNECT command servers

<table>
<thead>
<tr>
<th>PROD</th>
<th>SSID</th>
<th>S</th>
<th>SERVER NAME</th>
<th>SSID COLL_ID</th>
<th>NICKNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>DBBF</td>
<td>S</td>
<td>DBBA</td>
<td>DBBA ACTvr_D_MAIN</td>
<td>DBBFDDBBA*</td>
</tr>
<tr>
<td>ACT</td>
<td>DBBF</td>
<td>S</td>
<td>DBDB</td>
<td>DBDB ACTvr_D_MAIN</td>
<td>DBBFDDBB*</td>
</tr>
</tbody>
</table>

3. Update the values for the Server Name, Server SSID, and the Server Nickname.

4. Complete the instructions in the comment block of Figure 20 on page 192 to enable the servers that were added by the MSSID installation. These server entries will be commented out. Some editing of the new server entries might be required.

Figure 20: Control table for multiple SSID installation

* * * * * * * * * * * * * * * * * * * * * * * * *
* **INSERTED FROM MSSID INSTALL** *
* TO USE, MANUALLY UPDATE SERVER DATA ROWS BELOW *
* AND UNCOMMENT BY REMOVING COLUMN ONE ASTERISKS *
*PROD SSID S SERVER NAME       SSID COLL_ID     NICKNAME *
*------|------|-----|------------------|------------------|----------|
| ACT   | DBBF | S   | DBBA             | DBBA ACTvr_D_MAIN| DBBFDDBBA* |
| ACT   | DBBF | S   | DBDB             | DBDB ACTvr_D_MAIN| DBBFDDBB* |
| *ACT  | DBBA | S   | DBBA             | DBBA ACTvr_D_MAIN| DBBFDDBA* |
| *ACT  | DBBA | S   | DBDB             | DBDB ACTvr_D_MAIN| DBBFDDBB* |
| *ACT  | DBBA | S   | DBDA             | DBDA ACTvr_D_MAIN| DBBFDDBA* |

5. Press END to exit.

6. If either of the following conditions exists, type GENERATE on the COMMAND line:

- You edited the BMCD2 CLIST to use a generated permanent ISPF table for the control table (specified GENTABLE=Y in the BMCD2 CLIST)

- You modified the control table that was previously generated

   This action rebuilds the ISPF control table in the HLQUBMCTLIB data set.
Adding ACTEMAIN and ACTDCL to the ISPF command table

System security can use a TSO command-limiting function to restrict an individual user or an entire site. This function applies to TSO commands that are issued from the READY prompt or from ISPF.

To add commands to the ISPF command table

1. Edit the ISPF command table.

2. If command limiting is active, you must add the following commands to the list of commands that are allowed for CATALOG MANAGER:
   - ACTEMAIN—used to access CATALOG MANAGER
   - ACTDCL—used to create a DCLGEN in CATALOG MANAGER

Command limiting is activated in the following ways:

- For an individual, with the TSOCMDS field of the logon ID record
  TSOCMDS specifies the name of a module that contains a list of valid commands for a user. For a sample list, see the ACF$CMDS member of CAI.CAIMAC.

- For an entire site, with the CMDLIST field of the GSO record named TSO
  The ALLCMDS field indicates permission for a user to bypass command limiting. Use the character that is specified in the BYPASS field of the GSO TSO record as a prefix for the command name.

Enabling the use of DDF

CATALOG MANAGER and CHANGE MANAGER can access remote DB2 subsystems using the DB2 Distributed Data Facility (DDF). If you did not enable the use of DDF during the installation of the products, use the following procedure to enable DDF.

1. Edit the HLQ.UBMCCNTL member T1S#CDBS:
   a. Change the following variables to the values that you used when you installed CATALOG MANAGER or CHANGE MANAGER. To review the values, see the prdINIT5 or prdINIT6 member in the HLQJCL library (where prd is the product code). For CHANGE MANAGER, also review the values for Common SQL in the ACSINIT5 or ACSINIT6 member.
      - Replace **AUTHID with the value for the primary or secondary authorization ID.
- Replace **SQLID with the value of the alias qualifier.
- Replace **COLLID with the value of the collection ID.

b  *(CHANGE MANAGER)* For the aliases that are prefixed with CAT2 and CAT3, uncomment the SQL statements and add a dash (-). (That is, change *SQL to -SQL.)

c  *(CHANGE MANAGER)* If you are executing the worklist for only CHANGE MANAGER, comment out the BIND statements for the CATALOG MANAGER packages.

d  In the last SQL statement, specify to grant EXECUTE authority to PUBLIC or to specific users.

e  If you are executing the worklist for both CATALOG MANAGER and CHANGE MANAGER, repeat step Step 1.d on page 194.

2 Edit the $740INST job to create a single step to execute the T1S#CDBS worklist for CATALOG MANAGER and for CHANGE MANAGER.

3 Edit the BMCDB2 CLIST:

a  Edit the control table.

b  Specify the servers to use with CATALOG MANAGER CONNECT.

The same release level of CATALOG MANAGER must be installed on the remote DB2 subsystems and the DB2 subsystem from which you want to connect. The example in Figure 21 on page 194 shows that when CATALOG MANAGER is invoked on the DB2P subsystem, it can connect with the DB2A, DB2B, and DB2C servers on remote DB2 subsystems. In this example, the unique nicknames combine the server name and SSID.

<table>
<thead>
<tr>
<th>*PROD</th>
<th>SSID</th>
<th>SERVER NAME</th>
<th>SSID COLL_ID</th>
<th>NICKNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>DB2P</td>
<td>S DB2A</td>
<td>DB2A ACTvr_D_MAIN</td>
<td>DB2PDB2A</td>
</tr>
<tr>
<td>ACT</td>
<td>DB2P</td>
<td>S DB2B</td>
<td>DB2B ACTvr_D_MAIN</td>
<td>DB2PDB2B</td>
</tr>
<tr>
<td>ACT</td>
<td>DB2P</td>
<td>S DB2C</td>
<td>DB2C ACTvr_D_MAIN</td>
<td>DB2PDB2C</td>
</tr>
</tbody>
</table>

c  Press END to exit.

### Specifying minimum TSO region size

ALTER, CHANGE MANAGER, DASD MANAGER PLUS, BMC Workbench, and CATALOG MANAGER require that you configure a TSO region size of 32 MB or greater for each user who signs on.
Specific DASD MANAGER PLUS customization tasks

In addition to the customization tasks for multiple products and for the Administrative products, you will need to perform customization tasks for DASD MANAGER PLUS.

Enabling REXX executables

The Installation System generates REXX executables for DASD MANAGER PLUS. These REXX executables can be implicitly executed. Use the following procedure to enable the REXX executables:

1. To enable the REXX executables to be implicitly invoked from TSO without having to invoke DASD MANAGER PLUS, perform one of the following tasks:
   - Add the HLQ.UBMCCLIB library to your SYSEXEC concatenation.
   - Copy the REXX executables from the HLQ.UBMCCLIB library to a library in your SYSEXEC concatenation.

Customizing the ISPF-Export utility for DASD MANAGER PLUS

This section describes additional customization tasks that you need to complete to use the Export utility for DASD MANAGER PLUS.

With the Export utility, you can ensure that your DASD MANAGER PLUS object definitions match on all DB2 subsystems where DASD MANAGER PLUS resides. You can copy definitions from a local controlling DASD MANAGER PLUS repository to destination DASD MANAGER PLUS repositories on other DB2 subsystems. The subsystems can reside in the same sysplex or across sysplexes.

Before launching the Export from DASD MANAGER PLUS, review the tasks in “Preparing your environment for exporting” on page 201.

Recommendations for setting up connections

BMC recommends that you use one DB2 subsystem as your control or master subsystem. You can copy (export) all definitions from the control subsystem.
BMC also recommends using a primary UIM server as the connection repository. The UIM server is a TCP/IP application that facilitates communication between logical partitions (LPARS), which can span sysplexes. The UIM server provides the data transport mechanism between the source and destination.

Following these recommendations helps you avoid accidentally overwriting object definitions and connection information.

**Note**

To delete definitions from multiple data sources, you must manually delete the definitions from each data source.

## Connection list types

You must define at least one host connection when you launch the ISPF Export utility. You can then add and work with DB2 data sources. Defined host connections remain available each time you start the ISPF Export utility and log in. All host connections reside on the UIM server.

The ISPF Export utility supports the following types of connection lists:

- **Enterprise connection list (ECL)**
  
  An ECL is a shared list used to identify, using host and port information, the host connections that you define.

  The ECL contains host and port information for one or more UIM servers.

  **Note**

  - Administration: One or more administrators maintain the ECL. Users with appropriate authority can add, delete and edit ECL connection information.

  - The ECL does not contain DB2 subsystem information. Consequently, the ECL cannot be used as an Export destination. The ECL is more commonly used for IMS connections. From a DB2 perspective, you can use ECL as a seed value to create a PCL or CCL. The PCL and CCL do contain DB2 subsystem information and can be used as Export destinations.

- **Personal Connection List (PCL)**
  
  The PCL is a host connection for personal use. Separating personal connections from host connections makes it simple to isolate activities in different environments (such as testing systems and production systems or different groups of application systems). The PCL cannot be shared.
Common Connection List (CCL),

The CCL is similar to PCL, but can be shared. You can obtain all destinations from your PCL or CCL. To define PCL or ECL, enter the connection information (host name, port and DB2 subsystem ID). If your administrator has set up an ECL, you can create a PCL or CCL from an ECL by adding the DB2 subsystem ID information.

**Required authorizations for using ISPF-Export**

Before launching Export from DASD MANAGER PLUS, you need to appropriate Resource Access Control Facility (RACF) authority and SAF authority to access the ECL.

**TCP/IP and UIM server access**

Export uses existing login credentials for the definition phase. Export also prompts you for login credentials when you specify a UIM connection for the primary UIM server, and for any other UIM servers that will participate in an export. Export requires a valid RACF or equivalent user ID and password for these credentials. The security administrator for your site sets up the user ID and password.

The RACF security administrator must define an Open Multiple Virtual Storage (OMVS) segment for the UIM server started task in order to enable TCP/IP access. The security administrator must also assign a user ID with an OMVS segment to the started task procedure name for the UIM server address space.

The UIM Primary Server is the connection repository where PCL’s and ECL’s are stored. Communication to the primary UIM server is through the use of POF values for host name and port number. The security administrator usually specifies this information during installation.

When you launch Export, the JCL Generation component of DASD MANAGER PLUS accesses the POF to retrieve the primary UIM host name and port number. Export then prompts you for a TSO userid and password and creates a UIM connection using the host and port number specified in the POF.

---

**Note**

Typically, the security administrator sets the primary server value in the ASU_XP_UIMSRVHOST option before you launch Export. If that option was not set, Export uses the current system where you are logged in as the primary UIM server.

The following table lists the POF keywords that are associated with Export and specifies how they affect DASD MANAGER PLUS.
Table 99: POF keywords for specifying the UIM host definition

<table>
<thead>
<tr>
<th>POF keyword</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASU_XP_LOGD_DATAC=</td>
<td>Specifies the SMS data class and the allocation attributes of the Export log file</td>
</tr>
<tr>
<td>ASU_XP_LOGD_MGMTC=</td>
<td>Specifies the SMS management class that defines the migration, retention, and backup requirements of the Export log file</td>
</tr>
<tr>
<td>ASU_XP_LOGD_PRIQTY=10</td>
<td>Defines the primary allocation for the Export log file</td>
</tr>
<tr>
<td>ASU_XP_LOGD_SECQTY=2</td>
<td>Defines the secondary allocation for the Export log file</td>
</tr>
<tr>
<td>ASU_XP_LOGD_STORC=</td>
<td>Specifies the SMS storage class that defines the processing requirements of the Export log file</td>
</tr>
<tr>
<td>ASU_XP_LOGD_UNIT=SYSDA</td>
<td>Specifies the unit for the Export log file</td>
</tr>
<tr>
<td>ASU_XP_LOGDSN=&amp;PREFIX..XPORT.LOG(R)</td>
<td>Specifies the Export log file</td>
</tr>
<tr>
<td>ASU_XP_UIMSRVPORT=</td>
<td>Specifies the port number of the primary UIM server that contains the host definitions repository for the Export utility</td>
</tr>
<tr>
<td>ASU_XP_UIMSRVHOST=</td>
<td>Specifies the host name of the primary UIM server for the Export utility</td>
</tr>
<tr>
<td>ASU_XP_UIMSRVTIMEOUT=300</td>
<td>Specifies the UIM timeout parameter that determines how long the Export utility should wait for a response from the UIM server before timing out</td>
</tr>
</tbody>
</table>

TCP/IP and user access

An OMVS segment must be defined in RACF for each Export user ID. An OMVS segment is required to make use of TCP/IP services such as the FTP server on z/OS. The OMVS segment specifies the UIM to be used, the home directory, and the shell program name.

SAF authority to access the CCL

When defining Export destinations, one or more administrators can set up and manage a shared list of connections. If you make the shared list available to other users, they do not have to define their own PCLs.

Users with appropriate authority can modify information in the ECL and CCL. The security administrator sets the authority levels that enable users' access to and editing privileges for these connections. Table 100 on page 199 displays the available authority levels and their explanations.
Table 100: Authorization to edit the ECL or CCL

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>You must set up your own connections. You cannot view or edit the ECL or CCL.</td>
</tr>
<tr>
<td>READ</td>
<td>You can view and select connection definitions from the ECL or CCL.</td>
</tr>
<tr>
<td>UPDATE</td>
<td>You can view, edit, delete, and add connection definitions in the ECL or CCL.</td>
</tr>
</tbody>
</table>

In addition, the SAF provides an interface to your security product (for example, Computer Associates ACF, eTrust CA ACF2 Security for DB2, or eTrust CA Top Secret for DB2). SAF determines who can access z/OS resources, and at what levels, by using security rules. You can use SAF to define who can read or maintain the ECL based on:

- User ID
- Product function or feature

**Protection of access controls**

During installation of console-enabled products, the product does not prompt you to implement access controls. The product does prompt you to define address spaces for the UIM server and any other servers that are installed. Files in the server address space determine server configuration.

**UIM server configuration**

The UIM server configuration file SMF$DHSP is an XML configuration file that is used to implement access controls. The file is installed in the UIM server configuration data set (default data set name HLQ.CONFIG) on the mainframe.

To protect access control policy from unauthorized changes, you must secure update access to the XML configuration file. Doing so protects defined resource names from being substituted.

**Figure 22 on page 199** displayed the format that is used in the XML configuration file for specifying access controls. The format includes the name of the rule, the name of the resource, and the SAF class.

**Figure 22: Console configuration file excerpt**

```xml
<rule name="SDBA_DNA_EDIT_CONNECTION_LIST"
      resource="BBM.SDBA.DNA.ECL"
      class="FACILITY" />

<rule name="BBM.SDBA_DNA_EDIT_CCLCONNECTION_LIST"
      resource="BBM.SDBA.DNA.CCL"
      class="FACILITY" />

<rule name="SDBA_DNA_SPOOL"
      resource="SDBA_DNA_EDIT_CONNECTION_LIST"
      class="FACILITY" />
```
Creation of SAF resources

You can base the SAF resources that you create on the following elements:

- User ID
- Product function or feature

The following access types are predefined:

- **ACL_Full**—Access Control List Read/Write/Alter
  
  Users can:
  - Reference the CCL in the Select Export Destinations dialog
  - Manage Destinations
  - Administer the CCL (add, delete and update connections)

- **ACL_Write**—Access Control List Read/Write
  
  Users have the same access as ACL_Full.

- **ACL_Read**—Access Control List Read only
  
  - Users can reference the CCL in the Select Export Destination dialog.
  - Users cannot manage Destinations.

- **ACL_None**—Access Control List none
  
  CCL is not used. Export reverts to the PCL. Individual users manage their own connection lists.

  The rule name SDBA_DNA_COMMON_CONNECTION_LIST was not found in the SMF$DHSP member.

SAF uses classes to simplify security access implementation. When you create SAF resources, BMC recommends that you use the predefined FACILITY class. To use a different class, you must edit the XML configuration file HLQ.CONFIG(SMF$DHSP) attributes. The class name that is defined to SAF must be the same as the class name attribute in the XML configuration file. The XML configuration file should be protected from UPDATE access after installation to prevent a user from bypassing access controls.

**SAF resource definition for the console**

SAF resource definitions for the console use the naming pattern BBM.SDBA.*.*.*

BBM.SDBA is the high-level qualifier to define resources. The asterisks represent additional product-specific qualifiers. The number of low-level qualifiers is product specific. The following table shows how to access resource types.
Table 101: Access to resource types

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Specify this definition</th>
<th>To create a SAF resource that controls access to this resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECL</td>
<td>BBM.SDBA.DNA.ECL</td>
<td>ECL</td>
</tr>
<tr>
<td>CCL</td>
<td>BBM.SDBA.DNA.CCL</td>
<td>CCL</td>
</tr>
<tr>
<td>SPOOL</td>
<td>BBM.SDBA.DNA.JOBVIEW.SPOOL</td>
<td>JES queue viewer</td>
</tr>
<tr>
<td>SPOOL</td>
<td>BBM.SDBA.DNA.JOBMASK.SPOOL</td>
<td>Filter for the jobs that are displayed in the JES viewer</td>
</tr>
</tbody>
</table>

**Note**
If any of these resources (for example, RACF or ACF2) are not defined to your security system, all users have unrestricted access to the function that invokes the undefined resource.

### Preparing your environment for exporting

Use the following procedure to set up your environment to accommodate exporting definitions.

**Before you begin**

- Ensure that you have DASD MANAGER PLUS installed on each LPAR and configured for each DB2 subsystem that will participate in the export.
- Verify with the security administrator that TCP/IP access is enabled.

**To prepare your environment for exporting**

1. Verify that the UIM server that contains the connection repository (as well as each z/OS image that will participate in the export) is running by checking the JESMSGLG SYSOUT file for the following messages:

   ```text
   BMC3402901 UIM Server, Level v.r.mm mm,dd,yy, initialization complete!
   BMC3401221 Ready for MVS Operator Commands
   ```

2. Specify a primary UIM server by using the following POF keywords to specify the host name and port number:

   - `ASU_XP_UIMSRVPORT`
   - `ASU_XP_UIMSRVHOST`

3. *(optional)* Limit update access to the ECL (which contains all the connection information for the enterprise) by specifying the following definition:
Use this profile name with the RESOURCE CLASS of FACILITY to maintain users who can control the ECL.

Specifying minimum TSO region size

ALTER, CHANGE MANAGER, DASD MANAGER PLUS, BMC Workbench, and CATALOG MANAGER require that you configure a TSO region size of 32 MB or greater for each user who signs on.

Customizing Cross-System Image Manager (XIM)

The customization process constructs the XIM started task procedure and the XIM initiator procedure in the HLQ.JCL data set. Configuring XIM involves copying these procedures into the appropriate libraries. This procedure applies only to Database Administration and Object Administration solutions.

Before you begin

Complete the following tasks before you perform these customization tasks:

- Apply the appropriate component fixes.
- Submit all applicable installation jobs.

To customize XIM

1. Copy the XIM started task procedure from the HLQ.JCL data set into a procedure library that is recognized by your JES subsystem.

   Note
   The default name of the XIM started task procedure in the HLQ.JCL data set is XIMACM.

2. Specify the SUFFIX parameter (within the XIM started task procedure) that XIM receives as part of the XIM parameter options member name.

   The SUFFIX parameter identifies the last one to five characters of a partitioned data set (PDS) member that begins with the character string XIM (XIM xxxxx).
3 Copy the XIM initiator procedure from the HLQ.JCL data set into a procedure library that is recognized by your JES system.

**Note**
The default name of the XIM initiator procedure in the HLQ.JCL data set is either the name that you entered as the value for the INIT_PROC option or the default of XIMACMI.

You do not need to specify a valid SSID parameter within the XIM initiator procedure. XIM generates this value internally.

Do not include a STEPLIB DD statement in your initiator procedure. If you include this statement, you can encounter abends in the initiator.

### Execution of XIM

The Database Administration and BMC Object Administration for DB2 use the XIM technology to manage units of work (UOWs).

XIM executes as a separate OS/390 or z/OS started task. You must start XIM on each image where CHANGE MANAGER will use XIM as a distribution point for UOWs. XIM uses the services of the IBM Cross-System Coupling Facility (XCF) to locate and connect to other instances of itself within the OS/390 or z/OS parallel sysplex.

If your site uses the Resource Access Control Facility (RACF) or CA-Top Secret, you can authorize the procedures for the XIM subsystem as started tasks in the started procedures table. If your site uses CA-ACF2, you can authorize the procedures for the XIM subsystem as started tasks under the started task control. Table 102 on page 204 describes authorization for XIM.
Table 102: Authorizing XIM procedures

<table>
<thead>
<tr>
<th>Product</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACF or CA-Top Secret</td>
<td>Authorize the procedures for the following subsystems as started tasks in the started procedures table:</td>
</tr>
<tr>
<td></td>
<td>■ XIM performance subsystem</td>
</tr>
<tr>
<td></td>
<td>■ XIM extended job entry subsystem</td>
</tr>
<tr>
<td></td>
<td>If you are running RACF version 2.1 or later, you can use the STARTED class to add or modify RACF security definitions for started procedures without having to perform an IPL of the system. The STARTED class allows you to modify the security definitions dynamically through the RDEFINE, RALTER, and RLIST commands. For more information about using the STARTED class, see the appropriate RACF publication.</td>
</tr>
<tr>
<td>CA-ACF2</td>
<td>Authorize the procedures for the following subsystems as started tasks under the started task control:</td>
</tr>
<tr>
<td></td>
<td>■ XIM performance subsystem</td>
</tr>
<tr>
<td></td>
<td>■ XIM extended job entry subsystem</td>
</tr>
<tr>
<td></td>
<td>See the appropriate CA-ACF2 publication for more information.</td>
</tr>
</tbody>
</table>

Your systems programmer can issue XIM console commands from an OS/390 or z/OS console to start, stop, and modify XIM. This section describes the commands to use and the procedures to follow to perform the following tasks:

- Determine the status of XIM
- Start XIM
- Inactivate XIM initiators
- Shut down XIM
- Activate XIM initiators
- Modify MVS image variables
- Troubleshoot the execution of XIM

For more information about XIM, see the *Cross-System Image Manager User Guide*. 
Determining the status of XIM

You can use the STATUS command to display information about XIM instances in the sysplex or jobs connected to an XIM initiator.

To determine the status

1. To determine whether XIM is running, issue the following command:

   `/F XIMACM, STATUS`

An excerpt from the JES log shows the result of issuing the STATUS command where XIM is active:

<table>
<thead>
<tr>
<th>BMC951001</th>
<th>XIM STATUS Command Accepted, XIM STATUS in progress XIMACM</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC951811</td>
<td>STATUS, 3 XIM Members(s) ACTIVE in XIM Group XIMACM XIMACM</td>
</tr>
<tr>
<td>BMC951591</td>
<td>Jobname  Jobid    SmfId  Cvtsname Status</td>
</tr>
<tr>
<td>BMC951841</td>
<td>XIMACM   STC01000 DB2A  DB2A     Active    16 inits    0 active</td>
</tr>
<tr>
<td>BMC951841</td>
<td>XIMACM   STC08798 SYSN  SYSN     Active    16 inits    0 active</td>
</tr>
<tr>
<td>BMC951841</td>
<td>XIMACM   STC08638 DB2B  DB2B     Active    16 inits    0 active</td>
</tr>
</tbody>
</table>

Starting XIM

Start XIM on each OS/390 or z/OS image that processes work for CHANGE MANAGER.

Before you begin

Before you start XIM, ensure the following items:

- The STEPLIB library is APF authorized
- The XIM started task name is unique for each version of the solution if both of the following conditions exist:
  - You have installed the worklist parallelism feature of the Database Administration solution in one environment (for example, production).
  - You later install a new version of the solution in a different environment (for example, test).
- the XIM started task procedure name that is specified on the Execution Worklist Parallelism Options panel matches the name of the started task

For information about specifying the procedure name, see the ALTER and CHANGE MANAGER for DB2 User Guide, Volume 2.
To start XIM

1 To start XIM, issue the following command:

/S XIMACM

XIMACM is the name of the started task. The XIMACM procedure is located in a system PROCLIB data set. (When the component was installed, the procedure should have been copied to this data set.)

Under the following conditions, the Execution function of the solution attempts to start XIM automatically on the image on which Execution is running:

■ XIM is not started.

■ You attempt to execute a worklist that has worklist parallelism enabled.

■ The XIMSTART YES parameter is specified in the AEXPIN input stream in the execution JCL for a worklist.

XIM is not started on any image other than the image on which you submitted a job.

Inactivating XIM initiators

You can use the QUIESCE command to prevent additional work from being accepted. Work that is in progress is allowed to finish. Typically, you would issue this command before shutting down XIM.

To inactivate the initiators

1 To inactivate the XIM initiators, issue the following command:

/F XIMACM,QUIESCE

An excerpt from the system log shows the result of issuing the QUIESCE command:

BMC951001 XIM QUIESCE Command Accepted. XIM QUIESCE in progress XIMACM
BMC951001 XIM STOP Command Accepted. Initiator termination in progress
BMC985221 Initiator shutdown request received in ASID(01F6). XJS1
BMC982121 XJS initiator ended in ASID(01F6). XJS1

Note
The XIM initiators are inactivated only on the image on which you issued the QUIESCE command. If more than one image is participating in a group, issue the QUIESCE command on each image.
Shutting down XIM

You can use the SHUTDOWN command to terminate inactive XIM initiators and XIM.

Before you begin

Before you issue the command, inactivate all XIM initiators. If any XIM initiators are active, the SHUTDOWN command fails.

To shut down XIM

1. Issue the QUIESCE command.
2. To terminate the XIMACM address space completely, issue the following command on each image:

/F XIMACM,SHUTDOWN

Activating XIM initiators

If XIM is quiesced, you can use the ACTIVATE command to allow initiators to be scheduled again.

To activate initiators

1. To restart the XIM initiators, issue the following command:

/F XIMACM,ACTIVATE

Modifying MVS image variables

To modify variables that are specific to an OS/390 or z/OS image, you can modify the member from which active parameters are loaded.

Before you begin

Before you can modify the variables, you must determine the location from which the parameters are loaded.
To determine the location from which the parameters are loaded

1 Using your normal method to review SYSOUT, review the active XIMACM started task.

   Alternatively, you can review the XIMACM procedure in your system PROCLIB library.

2 Locate the partitioned data set (PDS) that is allocated to the XIMPARM ddname.

3 On the //EXEC PGM=XIMMAIN statement, locate the PARM option.

   A keyword specifies SUFFIX=xxxx.

4 To determine the member name, append the SUFFIX to XIM.

   For example, if SUFFIX=PARM, the active parameters are loaded from the XIMPARM member, as shown in the following line of JCL:

   ```
   //XIMPARM DD DSN=RCDTJP.XIM.UDBPARM(XIMPARM)
   ```

To modify the variables

1 Edit the XIM xxxx member in the data set that is referenced by the //XIMPARM DD statement.

   In the example shown in Figure 23 on page 209, the name of the member is XIMACMI.

2 Modify the INITIATORS variable.

   In the example shown in Figure 23 on page 209, the member contains global variables and MVS image variables. The variables in the MVS image variables section override the same variables in the global variable section. For example, the default value for the global number of initiators is 8. However, for the DB2A subsystem ID, the number of initiators is 16.
Note

Typically, you should not modify other variables unless Customer Support directs you to do so. However, you must ensure that the values for the XIM_GROUP and XCF_GROUP parameters are unique for each version if both of the following conditions exist:

- You have installed the worklist parallelism feature of the Database Administration solution in one environment (for example, production).
- You later install a new version of the solution in a different environment (for example, test).

In addition, the XIM group name that is specified on the Execution Worklist Parallelism Options panel must match the name of the group.

For information about specifying the group name, see the ALTER and CHANGE MANAGER for DB2 User Guide Volume 2.

Figure 23: XIMACMI member

```
* XIM STARTUP PARM FOR CHANGE MANAGER FOR DB2
*
* SYNTAX RULES:
* USE COL 1 - 71
* USE ONE PARAMETER PER STATEMENT
* DO NOT CONTINUE A PARM ONTO A SECOND LINE
* ANYTHING FOLLOWING A PARM AND ITS VALUE IS A COMMENT
* THE EQUAL SIGN IS THE REQUIRED DELIMITER
* SPACES TO THE LEFT AND RIGHT OF THE = ARE PERMITTED
* BLANK LINES AND LINES BEGINNING WITH * ARE IGNORED
* **************************************************************
*   GLOBAL VARIABLE SECTION         ******************
XIM_GROUP=XIMACM
XCF_GROUP=XIMACMCF
INITIATORS=8
INIT_PROC=XIMACMI          *  PROC FOR TARGET INITIATORS
*
* RESPONSE TIMEOUT INTERVAL (SECONDS)
RESPONSE_TIMEOUT=90        *  RESPONSE TIME OUT (SECONDS)
WORKLOAD_REFRESH=1          *  WORKLOAD REFRESH INTERVAL (MINUTES)
ENVIRONMENT_TIMER=60        *  ENVIRONMENT TIMER INTERVAL (SECONDS)
*
* LOCAL MVS IMAGE VARIABLES (COMMENTED TO SHOW AS AN EXAMPLE)
* DO DB2A
* INITIATORS=16        *  # OF INITIATORS AT STARTUP
* END
```

3 Save the changes to the member.

4 Inactivate XIM by issuing the QUIESCE command:

```
/F XIMACM,QUIESCE
```

5 Verify the status of XIM by issuing the STATUS command:

```
/F XIMACM,STATUS
```
6 Shut down XIM by issuing the SHUTDOWN command:

/F XIMACM,SHUTDOWN

7 Start XIM by issuing the start command:

/S XIMACM

The new instance of XIMACM uses the new parameters.

8 To verify the new parameters, issue the STATUS command:

/F XIMACM,STATUS

9 Review the values that XIM displays in the system log.

10 If you use data sharing, repeat Step 4 on page 209 through Step 9 on page 210 for each OS/390 or z/OS image.

**Troubleshooting the execution of XIM**

Use the following procedure if your job could not connect with XIM.

**To troubleshoot XIM**

1 Use any of the following methods to determine why a job failed to connect to XIM:

- Issue the STATUS command to verify whether XIM was started:
  
  /F XIMACM,STATUS

- If you are using a data sharing environment, ensure that XIM was started on all of the images.

- Ensure that the STEPLIB library was APF authorized.

- Review the output from the XIMACM started task procedure.

- Review the XIM job or the system log for error messages that were issued by the XIM started task or by the CHANGE MANAGER batch job.

  Using your job name, search the log for enqueue-type messages for the IBM Global Resource Serialization (GRS) or Unicenter CA-MIM products.

  If you are using a data sharing environment with multiple OS/390 or z/OS images and you previously canceled a parallel job, an initiator might still be
running and holding data sets. This initiator might be preventing another initiator from starting.

- If necessary, specify the TRACE YES keyword in the AEXPIN input stream and run the job again.

For more information, see the *ALTER and CHANGE MANAGER for DB2 User Guide, Volume 2*.

## Working with CLISTs

This section describes how to work with CLISTs.

### Using the appropriate CLIST

If multiple versions of the products are installed and the version and release numbers of the products on one DB2 subsystem are later than the version and release numbers of the products on another DB2 subsystem, use the CLIST for the later version and release of the products.

**To use the CLIST**

1. Ensure that a current copy of the appropriate CLIST is in the same SYSPROC concatenated library as your other CLISTs.

For example, if you installed version 10.1 of CATALOG MANAGER on DB2 subsystem DBDA and you installed version 11.1 of CATALOG MANAGER on DB2 subsystem DBDB, and you want to use one CLIST, use the CLIST for version 11.1 of CATALOG MANAGER on DBDB.

The Installation System generates the CLISTs for the Administrative products that are listed in the following table.

### Table 103: CLISTs for the Administrative products

<table>
<thead>
<tr>
<th>CLIST</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTPSS</td>
<td>Defines the integration of CATALOG MANAGER and SQL Explorer for DB2</td>
<td>HLQUBMCCCLIB</td>
</tr>
<tr>
<td>AEXADMF1</td>
<td>Invokes Fast Path Navigation for the Administrative products</td>
<td>HLQUBMCCCLIB</td>
</tr>
<tr>
<td>AEXADMF2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CLIST</td>
<td>Description</td>
<td>Location</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>ALUWLDDL</td>
<td>Converts an ALTER or CHANGE MANAGER worklist to a DDL file</td>
<td>HLQ.BMCCLIB</td>
</tr>
<tr>
<td>ALUXGRNT</td>
<td>Creates an additional ALTER or CHANGE MANAGER worklist that contains -SETS and -SQL authorization commands only</td>
<td>HLQ.BMCCLIB</td>
</tr>
<tr>
<td>BMCDB2</td>
<td>Invokes the Administrative products</td>
<td>HLQ.UBMCCLIB</td>
</tr>
<tr>
<td>BMCDRIVC</td>
<td>Defines user libraries for the product driver panels</td>
<td>HLQ.UBMCCLIB</td>
</tr>
<tr>
<td>CKSQNUM</td>
<td>Enables you to verify SQL worklists sequencing for ALTER and CHANGE MANAGER</td>
<td>HLQ.UBMCCLIB</td>
</tr>
<tr>
<td></td>
<td>To use the CKSQNUM CLIST, copy it from your installation library to a CLIST library from which you can run it. The CKSQNUM CLIST is used outside the Installation System.</td>
<td></td>
</tr>
<tr>
<td>FIXSQNUM</td>
<td>Enables you to verify and fix SQL worklists sequencing for ALTER and CHANGE MANAGER</td>
<td>HLQ.UBMCCLIB</td>
</tr>
<tr>
<td></td>
<td>To use the FIXSQNUM CLIST, copy it from your installation library to a CLIST library from which you can run it. The FIXSQNUM CLIST is used outside the Installation System.</td>
<td></td>
</tr>
<tr>
<td>POFRESET</td>
<td>For the Administrative products, enables you to reset all of the ISPF variables in the ISPF profile with the variables in the initial or user POF. The POFRESET CLIST is used outside the Installation System.</td>
<td>HLQ.BMCCLIB</td>
</tr>
<tr>
<td>RSTRIG</td>
<td>Calls the DASD MANAGER PLUS BMCTRIG Restart program</td>
<td>HLQ.UBMCCLIB</td>
</tr>
</tbody>
</table>

### Enabling the implicit execution of CLISTs

This procedure describes the steps that you must perform to enable the implicit execution of the CLISTs that are generated for ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS.

**To enable the implicit execution**

1. Enable the BMCDRIVC CLIST.
Copy the CLIST from the \textit{HLQ}JCL library or the \textit{HLQ}UBMCCLLIB library to a library in your SYSPROC concatenation.

2 \textit{(ALTER or CHANGE MANAGER)} Perform one of the following tasks to enable the ALTER or CHANGE MANAGER CLISTs (ALUXGRNT, ALUWLDDL, FIXSQSUM, and CHKSQNUM) to be implicitly invoked from within a worklist:

- Add the \textit{HLQ}BMCCLIB (ALUXGRNT or ALUWLDDL) library or the \textit{HLQ}UBMCCLLIB (FIXSQSUM or CHKSQNUM) library to your SYSPROC concatenation.

- Copy the CLISTs from the \textit{HLQ}BMCCLIB (ALUXGRNT or ALUWLDDL) library or the \textit{HLQ}UBMCCLLIB (FIXSQSUM or CHKSQNUM) library to a library in your SYSPROC concatenation.

3 \textit{(DASD MANAGER PLUS)} Perform one of the following tasks to enable the RSTRIG CLIST for DASD MANAGER PLUS to be implicitly invoked from within JCL:

- Add the \textit{HLQ}UBMCCLLIB library to your SYSPROC concatenation.

- Copy the CLISTs from the \textit{HLQ}UBMCCLLIB library to a library in your SYSPROC concatenation.

\textbf{Working with the BMCDB2 CLIST}

For the ALTER, CATALOG MANAGER, CHANGE MANAGER, and DASD MANAGER PLUS products, the Installation System generates an ISPF interface based on the options and components that you specify during installation. Products or components that are installed with different high-level qualifiers (for example, installed individually and residing in different libraries) can be accessed from the interface.

The interface consists of a CLIST (BMCDB2) and panels (BMCDB2PR, BMCDB2P2, BMCDB2TB, and BMCDB2H). You can use this combination without making changes to your TSO logon procedure. BMC recommends that new users use the supplied ISPF interface. The products or components require you to execute the CLIST from one of the ISPF dialog panels in your system.

The BMCDB2 CLIST uses the ISPF LIBDEF command to allocate all of the BMC product libraries. The Installation System customizes BMCDB2 and BMCDB2PR to include the data set names that you used when you installed the products or components. The Installation System specifies up to two DB2 load libraries and specifies the installation options module name for each product to support the DB2 subsystem where the component is installed.
If you install the products or components individually using the same target data sets, the BMCDB2 CLIST and BMCDB2PR panels are generated using the options only for the last product or component that was installed. Therefore, you might not be able to access the previously installed product or component unless you edit the BMCDB2 CLIST.

**Setting the variables in the BMCDB2 CLIST**

The BMCDB2 CLIST invokes the Administrative products. You can edit several variables in the BMCDB2 CLIST to specify libraries and to use a generated permanent ISPF table. This procedure describes how to modify the variables.

---

**Note**

To turn off the PF key display, issue the PFSHOW OFF command.

When you edit variables in the BMCDB2 CLIST to specify libraries, do not change the qualifier of the product data sets. Each of the data sets uses a designated qualifier that varies, depending on whether you use runtime, SMP/E, or user libraries.

---

**To set the variables in the CLIST**

1. To invoke the BMCDB2 CLIST implicitly, copy the CLIST from the HLQ.JCL library or the HLQ.UBMCCLIB library to a library in your SYSPROC concatenation.

2. Edit the BMCDB2 CLIST.

3. If you copied the BMCDB2 CLIST from the HLQ.JCL library or the HLQ.UBMCCLIB library to a library in your SYSPROC concatenation, modify the BMCDB2C variable in the BMCDB2 CLIST.

   Set this variable to the library in which the BMCDB2 CLIST was copied.

4. If you copied the BMCDB2PR, BMCDB2P2, BMCDB2TB, and BMCDB2H panels from the HLQ.JCL library or the HLQ.UBMCCLIB library to another library, modify the BMCDB2P variable in the BMCDB2 CLIST.

   Set this variable to the library in which the panels were copied.

5. To improve the performance of the invocation of the products from a large control table in the BMCDB2 CLIST, set the GENTABLE variable in the BMCDB2 CLIST to Y:

```
SET BMCDB2T = &STR(BMC.DB2ADMN.D91.UBMCTLIB) /* Control TABLE DATASET */
SET GENTABLE = Y /* USE GENERATED PERMANENT TABLE (Y/N) */
/* FOR Control TABLE */
```
To place a control table in a permanent ISPF table in the HLQ.UBMCTLIB data set, invoke the BMCDB2 CLIST (see “Invoking the BMCDB2 CLIST” on page 215).

6 To not use the TSO ALTLIB command to dynamically add libraries to the SYSPROC concatenation, set the ALTCLIST variable to N.

7 Press END to exit.

**Invoking the BMCDB2 CLIST**

Use the following procedure to invoke the BMCDB2 CLIST.

**To invoke the BMCDB2 CLIST**

1 Invoke the BMCDB2 CLIST by using one of the following commands:

   ■ Invoke BMCDB2 explicitly from your CLIST data set in the ISPF command shell or your ISPF dialog with the following command:

   ```
   EX 'HLQ.UBMCCLIB(BMCDB2)'
   ```

   ■ If the BMCDB2 CLIST is copied to a library in your SYSPROC concatenation, invoke BMCDB2 implicitly with the following command:

   ```
   %BMCDB2
   ```

   To specify various parameters with the BMCDB2 command, see “BMCDB2 command” on page 216.

2 If the BMCDB2 CLIST supports multiple SSIDs:

   a On the BMC Administrative Products for DB2 (BMCDB2PR) panel, type ? for the DB2 SSID

   b On the BMCDB2 Subsystem Selection List (BMCDB2P2) panel, type S to select an SSID from the list of available SSIDs.

   The SSID that you selected is displayed in the DB2 SSID field on the BMC Administrative Products for DB2 (BMCDB2PR) panel.

   c Press Enter.

3 If one of the following conditions exist, on the BMC Administrative Products for DB2 (BMCDB2PR) panel, type GENERATE on the COMMAND line:
You edited your BMCDB2 CLIST to use a generated permanent ISPF table for the control table by setting the GENTABLE variable to Y

You modified the control table that was previously generated

You want to specify the OPENTBL parameter in the BMCDB2 command

Issuing the GENERATE command places a control table in a permanent ISPF table in the HLPQ.UBMCTLIB data set, which improves the performance of the invocation of the products from a large control table referenced by the BMCDB2 CLIST. Refer to the BMCDB2T variable in the BMCDB2 CLIST for the location of the generated ISPF table.

4 Verify that all of the products appear on the BMCDB2PR panel that is displayed.

**BMCDB2 command**

This topic describes the parameters that you can specify with the BMCDB2 command.

You can specify various parameters with the BMCDB2 command to perform the following functions:

- Avoid the use of the ISPF LIBDEF facility to allocate the necessary ISPF data sets
- Use the ISPF LIBDEF facility to allocate all of the ISPF data sets, except the load data set
- Invoke the BMCDB2 CLIST implicitly
- Invoke a product implicitly
- Invoke ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS directly, without displaying the BMC Administrative Products for DB2 (BMCDB2PR) panel (improves performance)
**BMCDB2 command syntax**

The syntax of the BMCDB2 command is shown in the following figure.

**Figure 24: BMCDB2 command**

The parameters specify the following information:

- **LIBDEF**—determines whether the BMCDB2 CLIST should use the ISPF LIBDEF facility to allocate all necessary ISPF data sets (YES or NO)

  **Note**
  
  By default the BMCDB2 CLIST uses the ISPF LIBDEF facility to allocate all necessary ISPF data sets. Thus, you might not need to modify your TSO logon procedure to allocate data sets. If ISPF 4.2 or later is available, the STACK keyword is added to all LIBDEF statements that are used in the BMCDB2 CLIST.

- **LOADLDEF**—when LIBDEF is YES, indicates whether the ISPF LIBDEF facility should be used to allocate the ISPLLIB (load) data set (YES or NO)

  Use the LOADLDEF parameter if you have copied the load library for a product in your subsystem LINKLIST data sets or if you have previously added the load library to your STEPLIB concatenation.

- **CLSTEXEC**—indicates whether the BMCDB2 CLIST should be invoked explicitly (EXPLICIT) or implicitly (IMPLICIT)

  — If the CLIST is invoked explicitly, you must use a fully-qualified data set name and member name.

  — If the CLIST is invoked implicitly, you can use only the member name. In addition, the CLIST must reside in a library in your SYSPROC concatenation.
In previous releases, the CLSTEXEC parameter controlled the invocation both the BMCDB2 CLIST and ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS. The parameter now controls only the invocation of the BMCDB2 CLIST. To control the invocation of the products, use the LOADEXEC parameter.

- LOADEXEC —indicates whether the BMC products should be invoked explicitly (EXPLICIT) or implicitly (IMPLICIT)

The syntax of the BMCDB2 command display options is shown in the following figure.

**Figure 25: BMCDB2 command—display options**

The display option parameters specify the following information:

- PGM—specifies the name of the *program*, as listed in the following table

**Table 104: Program names**

<table>
<thead>
<tr>
<th>Product</th>
<th>program</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALTER</td>
<td>ALUFRONT</td>
</tr>
<tr>
<td>CATALOG MANAGER</td>
<td>ACTEMAIN</td>
</tr>
<tr>
<td>CHANGE MANAGER</td>
<td>ACMFRONT</td>
</tr>
<tr>
<td>DASD MANAGER PLUS</td>
<td>ASUFMAIN</td>
</tr>
</tbody>
</table>

- PROD—specifies the three-character product code (*prd*)
- CFUNC—specifies the CLIST function to perform (ALLOC)
- SSID—names the DB2 subsystem that is used to invoke the product (*ssid*)

**Note**
The SSID must be a valid DB2 subsystem that is defined in the control table.

- OPENTBL—specifies to issue an OPEN command against the control table (YES or NO)
**Note**
Before you can invoke a BMCDB2 command that specifies the OPENTBL(YES) option, you must first issue the GENERATE command from the BMC Administrative Products for DB2 (BMCDB2PR) panel.

- **BASEID**—no longer used
- **SHRAPPL**—indicates whether the products on a single SSID should use a shared ISPF profile (S) or use an individual profile (I)
- **ACCESS**—specifies to access the DB2 catalog directly (DIRECT) or to use an indirect copy of the catalog (INDIRECT)

**Examples**

The following examples show how you can use the various parameters with the BMCDB2 command.

**To avoid the use of the ISPF LIBDEF facility**

To avoid the use of the ISPF LIBDEF facility to allocate the necessary ISPF data sets, use the following command:

```
%BMCDB2 LIBDEF(NO)
```

**To use the ISPF LIBDEF facility for all data sets, except the load data set**

To use the ISPF LIBDEF facility to allocate all of the necessary ISPF data sets, except for the load data set, use the following command:

```
%BMCDB2 LIBDEF(YES) LOADLDEF(NO)
```

**To invoke the CLIST implicitly**

To invoke the CLIST implicitly, use the following command:

```
%BMCDB2 CLSTEXEC(IMPLICIT)
```

**To invoke ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS implicitly**

To invoke a product implicitly, use the following command:

```
%BMCDB2 LOADEXEC(IMPLICIT)
```
To invoke ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS directly

To invoke a product directly, you use the display options of the BMCDB2 command. When you use these options, the BMC Administrative Products for DB2 (BMCDB2PR) panel is not displayed. For example, to invoke CATALOG MANAGER directly, use the following commands:

```
%BMCDB2
GENERATE (from the BMC Administrative Products for DB2 [BMCDB2PR] panel)
ex 'HLQ.UBMCCLIB(BMCDB2)' 'PGM(ACTEMAIN) PROD(Act) SSID(DEBA) CFUNC(ALLOC) OPENTBL(YES)'
```
Customizing Backup and Recovery

This chapter describes additional customization tasks that are specific for the backup and recovery products.

Customizing RECOVERY MANAGER

You must customize RECOVERY MANAGER to operate in your environment.

Required temporary tables for RECOVERY MANAGER

RECOVERY MANAGER uses declared DB2 global temporary tables when performing the following tasks to generate recovery JCL:

- Multi-job optimization
- Stacked tape analysis
- Unchanged analysis (XUNCHANGED) processing for local subsystem recoveries
- Creating and reading groups from the repository

To ensure that you have enough space allocated for processing, set up the temporary tables. For DB2 Version 10 or later systems, DB2 uses the work file database to dynamically allocate the global temporary tables. For each DB2 Version 10 or later subsystem and for each member of a DB2 Version 10 or later data sharing system, you must ensure that the work file database contains at least one table space defined with a page size of 32 KB.

For information about creating the 32 KB table space in the work file database, see the documentation for IBM DB2 UDB for z/OS.
Preparing for archive logs greater than 64 KB tracks

To successfully use archive logs greater than 64 KB tracks, you must set up some SMS rules.

To set up SMS rules for large archive logs

1. Create an SMS DATACLAS that uses LARGE for the data set name type.

   This value assigns a DSORG type of PS-L to the data set. The simplest way to accomplish this is to make assignments based on a data set name filter, as in the following example:

   WHEN (&DSN = DSNDXW.DXW2.ARCLG1L.A0*)
   SET &DATACLAS = 'DCLARGE'

2. Create a DATACLAS rule to accommodate temporary files that some RECOVERY MANAGER programs create when processing archive logs.

   These files are identified with .Z0* and should also be allocated as DSNTYPE=LARGE. An example follows:

   WHEN (&DSN = DSNDXW.DXW2.ARCLG1L.Z0*)
   SET &DATACLAS = 'DCLARGE'

3. Because archive log and temporary files can be extremely large, set up a STORCLAS rule and a STORGRP rule to direct the data sets to a specific SMS storage group.

   Examples follow:

   WHEN (&DATACLAS = 'DCLARGE')
   SET &STORCLAS = 'DXWSMS'

   and

   WHEN (&STORCLAS = 'DXWSMS')
   SET &STORGRP = 'DXWSMS'

Setting up data sharing for RECOVERY MANAGER for DB2

If you have installed RECOVERY MANAGER for some of your DB2 subsystems and are now preparing to migrate to data sharing, use this procedure.
To set up data sharing for RECOVERY MANAGER

1. Add the following to the option set for each DB2 subsystem:

```
   groupname.DSNLOAD=DB2.load.library
   groupname.DSNEXIT=DB2.exit.library
   groupname.DSNLOAD=DB2.load.library
   groupname.DSNEXIT=DB2.exit.library
```

The variable `groupname` represents the group attach name of your data sharing group.

2. Verify that the following options are set in the option set for each DB2 subsystem:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>optionname</code></td>
<td>Options common to all subsystems</td>
</tr>
<tr>
<td><code>ssid. optionname</code></td>
<td>Options for each subsystem and data sharing member</td>
</tr>
</tbody>
</table>

3. For each DB2 subsystem that will be a data sharing member, use the **Product Option Sets** option on the RECOVERY MANAGER main menu to update the work file database name and the group member name.

RECOVERY MANAGER, LGC, and DBC

RECOVERY MANAGER, which is also part of the Recovery Management solution, uses DB2 Product Configuration (LGC) for maintaining product option sets. LGC runs as an agent within the DB2 Component Services (DBC) started task address space. The DBC started task must be started in order to run RECOVERY MANAGER.

For more information about LGC and DBC, see the *BMC Infrastructure Components Administration Guide*.

RECOVERY MANAGER *for DB2* archive history file

The RECOVERY MANAGER *for DB2* archive history file records all archive logs processed by the batch archive program, ARMBARC. You should create an archive history file for each DB2 subsystem on which disaster recovery procedures will be generated.

The archive history file is also used to record image copies of DSNDB01.DBD01, DSNDBD01.SYSUTILX, DSNDB06.SYSCOPY, and DSNDB01.SYSDBDXA. Recording |
these entries in the history file allows the batch system resource recovery program, ARMBSRR, to create efficient recovery JCL for all catalog and directory spaces.

If you specify a name for the archive history file during the installation, the installation jobs create the history table. If you do not create a table during installation, you can use the ARMHIST member in the DBCNTL data set to create and format one. The archive history will also be created when the ARMBARC program is executed.

**RECOVERY MANAGER for DB2 option set**

The ARM$OPTS, which is the default option set, contains information for all subsystems that share the RECOVERY MANAGER for DB2 load libraries and control files.

Adding a DB2 subsystem to RECOVERY MANAGER for DB2 adds the control information for that subsystem to the existing option set, ARM$OPTS.

If you browse the option set, you will see that variables unique to a DB2 subsystem are prefixed with the subsystem ID. Sharing the ARM$OPTS file among multiple subsystems could have repercussions for batch JCL generation processes. However, using the &SSID variable in the batch output JCL file name ensures that generated JCL can be easily identified and will not overlay JCL generated for other DB2 subsystems.

For more information, see the *RECOVERY MANAGER for DB2 User Guide*.

**RECOVERY MANAGER for DB2 packages**

RECOVERY MANAGER for DB2 packages are versioned with an ISO timestamp. SYSPACKAGE in the DB2 catalog will need to be cleaned up by using the FREE command because each release of RECOVERY MANAGER introduces a new version of each package.

**RECOVERY MANAGER for DB2 repository**

The repository consists of a set of table spaces that contain tables holding information about the groups that you create, including their attributes, subsystem, and group options.
A repository is required for each DB2 subsystem. In a data sharing environment, one repository is required for each data sharing group.

**BCSS commands for PACLOG**

The following commands are used to initialize the product in PACLOG processing only (PPO) mode. The REINIT PPO command is used to reinitialize PPO mode.

```
DAC ELM value
DAC LCO ON
DAC STATUS
REINIT PPO
```

After the REINIT PPO command is issued, the following commands are executed automatically:

```
DAC NVSAM ENABLE
DAC PPO ON
DAC PPO SHUTDOWN
```
Customizing System and SQL Performance

This chapter describes additional customization tasks that are specific for the System and SQL Performance products.

Overview

The System and SQL Performance products and solutions for DB2 provide an integrated environment that allows you to use one performance product or solution alone or multiple products or solutions together.

Using products together saves time and further automates performance analysis functions. The integrated environment from which the products operate allows all products to operate concurrently without placing unnecessary burdens on system storage, resource use, or execution time.

When multiple System and SQL Performance products or solutions are installed and active, they share a common interface. If multiple products are installed but only one product is active, the product-specific main menu for the active product is displayed instead of a common main menu. The main menu that is displayed reflects the active product mix.

Figure 26 on page 227 is an example of the main menu for a single product.

Figure 26: SQL Explorer main menu

```
DIY4 -------------------------- SQL EXPLORER vv.rr.mm -----------------------
Command ==>>
Option . . 0. Options
  1. Explain
  2. Explain and Compare
  3. Compare
  4. Mismatch Analysis
  5. Impact Analysis
  6. DBRM / Load Compare
  7. Migrate Access Path Statistics
  8. Declarations Generator
  9. SQL Explorer Rules Help
```
M. Maintenance
SSID . . . . . DIY4
DDF Location

Figure 27 on page 228 is an example of the main menu that is displayed when all System and SQL Performance products and solutions are installed and active.

Figure 27: System and SQL Performance for DB2 common main menu

DOMESEL/I System and SQL Performance for DB2 18:17:00
Command ====> ________________________________________________________________
Current Data Collector : A62D Status : ACTIVE
SELECT ONE OF THE FOLLOWING OPTIONS. THEN PRESS ENTER.
_ D. SYSTEM PERFORMANCE SOLUTION - DB2 SUBSYSTEM AND STORAGE POOL ANALYSIS
--- SQL PERFORMANCE SOLUTION ---
Q. APPTUNE AND INDEX COMPONENT - DB2 APPLICATION AND INDEX ANALYSIS
S. SQL EXPLORER COMPONENT - DB2 SQL ANALYSIS
A. PERFORMANCE ADVISORS - ADVICE AND RECOMMENDATIONS
1. DOMPLEXES - SELECT/CHANGE DOMPLEX CONNECTION
2. SESSION STATUS - VIEW CURRENT SESSION RESOURCE USAGE
3. USER OPTIONS - VIEW/MODIFY USER OPTIONS
4. LOG OPERATIONS - VIEW/PRINT LOGGED SCREENS AND REPORTS
5. ADMINISTRATION - MANAGE PRODUCT AND USER PROFILES
H. HELP
X. EXIT Z. ABOUT THE SYSTEM AND SQL PERFORMANCE PRODUCTS

Note
The MainView for DB2 - Data Collector component provides access to Administration functions of the System and SQL Performance products environment by a hyperlink from a MainView for DB2 Easy Menu. For more information, see the MainView for DB2 User Guide

Post-installation tasks

When you finish using the Installation System to generate and execute installation JCL, you must perform various post-installation tasks to complete the installation process. This section provides a detailed description of the post-installation tasks that are common to the System and SQL Performance products. Perform these tasks in the order in which they are presented. These tasks must be performed only once, even if you are installing multiple products.

1. Defining a DOMPLEX.
   If you are installing only SQL Explorer or OPERTUNE, this task does not apply.

2. Verifying the product for data sharing members.

3. Customizing the CLISTs for SQL Explorer and CATALOG MANAGER.
4 Creating indexes to improve performance.

5 Generating Help text from DB2 trace record field descriptions.

6 Editing or reviewing the DBC JCL procedure (DBC$STC).
   If you are installing only SQL Explorer or OPERTUNE, this task does not apply.

7 Adding or replacing the CLIST member for the ISPF interface.

8 Making products available from a menu.

9 Invoking SQL Explorer directly.

10 Invoking BMC Software products without LIBDEFs.

11 Verifying or changing the global resource enqueues.

12 Refreshing the MVS Linklist Lookaside.

13 Verifying the product authorization.

## Defining a DOMPLEX

This task applies to all System and SQL Performance products except OPERTUNE and SQL Explorer.

1 On the main menu for your System and SQL Performance product or solution, select **Administration**.

2 On the Administration menu, select 2 (DOMPLEX Option Sets).

3 On the DOMPLEX Options Set panel, perform the relevant action:

   - **If you migrated from a previous release**, the Installation System migrated your previous option set to the new release. The option set contains values that you specified in the install dialog.
     To review or edit the values, select the DOMPLEX option set.

   - **If you did not migrate from a previous release**, the Installation System created a DOMPLEX option set for you using values that you specified in the install dialog.
     To review or edit the values, select the DOMPLEX option set.
If the DOMPLEX option set that you want to use is not listed, type I to insert a new option set and press Enter.

4 On the DOMPLEX option set panel, expand each section and review or change the values.

**Tip**
To expand sections on the DOMPLEX option set panel, place the cursor on the + sign next to a section and press Enter. The major sections are DOMPLEX Parameters, Data Collector List, DB2 Monitor List, and Output Groups.

You must define at least one Data Collector, one DB2 subsystem to monitor, and one output group with LOGSET parameters. For more information about individual fields and sections, press F1 for Help or see the System and SQL Performance for DB2 Administrator Guide.

5 Press F3 when you finish.

6 If the product prompts you for a new option set, name the DOMPLEX option set and type a description.

**Note**
The DOMPLEX name should match the DOMPLEX value specified in the $480INIT job. The Data Collector name should match the DBC subsystem ID.

To define this DOMPLEX option set name to the DOM agent in the DBC, perform the following steps:

- a Rerun the DOMSTRT step of the $480INIT job to define the DOMPLEX option set name to the DOM agent in the DBC.
- b Review the DVDBCDPL variable in the $$INCINF member.

---

**Editing the DOMPLEX option set online**

Use this procedure to edit the DOMPLEX option set through the online interface.

**Note**
When working in the interface, you might need to type FILTOFF on the command line to see all of the fields.

1 In the interface, navigate to the DOMPLEX Options Set panel.

2 Select a DOMPLEX option set for modification by typing E in the field beside a DOMPLEX.
The panel displays sections in that option set:

| Filter: Off | Parameters that apply to entire DOMPLEX |
| + DOMPLEX Parameters | Data Collector(DBC) subsystems in DOMPLEX |
| + Data Collector List (1) | DB2 Sub-systems to be monitored |
| + DB2 Monitor List (11) | Output Groups - valid range: 001-256 |
| + OutGp DCID DspSize (6) |

**Tip**
You can expand a section by selecting the plus sign and pressing Enter, or by typing S over the sign. (To collapse an expanded section, select the minus sign and press Enter, or type S over the minus sign.)

3 Expand the **DOMPLEX Parameters** section, and ensure that you have the correct SECURITY and COPYDIR data sets listed.

This section contains values that apply to the entire DOMPLEX.

4 Expand the **Data Collector List** section, and ensure that the DBC ID is specified as the Data Collector.

This section lets you define the initialization parameters for each Data Collector (for example, the number of concurrent batch and online users allowed).

**Tip**
The **Data Collector List**, **DB2 Monitor List**, and **OutGp DCID DspSize** sections contain collections of repeating groups and support the following commands:
- I inserts a new instance in the repeating group.
- D deletes an instance.
- R replicates an instance.

5 *If you have a license that recognizes Pool Advisor*, perform the following steps:

a Expand the **Data Collector List** section.

b Open each Data Collector ID listed, and zoom into each of the following fields by putting your cursor on the > sign and pressing Enter:
- **Data Collectors advisor variable repository (DOMVARS)**
- **Pool Advisor history repository (PMDHIST)**
Note
When Pool Advisor starts, the Data Collector defines and allocates these two repository data sets with default values. If you need to correct the allocated default values, delete these data sets and then create and redefine new data sets (using the PMDHIST and PMDJINST members from the SAMP data set (BMCSAMP)). If you change the data set names, make sure to enter the new names in these two fields in the option set before you start the DOM agent.

6. Expand the **DB2 Monitor List** section, open each DB2 subsystem, and ensure that you have the correct Dynamic Explain plan name for this release. The default name is DAAvvrD1.

This section lets you identify and define the DB2 subsystems that Data Collectors in the DOMPLEX can monitor.

7. Expand the **Output Groups** section, open each output group, and check that the Data Collector SSID is correct and matches the DBC SSID that you plan to use on each LPAR in this sysplex for the same DBC group.

This section lets you define the output groups that will be used to buffer trace records, and to define and allocate log files that records are written to from the output groups.

---

**Note**

Do not use an asterisk (*) for the Data Collector ID. If you have a DB2 subsystem that comes up on different LPARs, define it to all of the Data Collectors that might monitor it.

8. Set the **NGL LOGSET** parameters:
   
   a. Expand the **LOGSET Parameters** section.
   
   b. Define a value for the **LDS Allocation type** and the appropriate SMS data.

   c. Ensure that a high-level qualifier (HLQ) is defined for the **NGL LDS DSN prefix**.

<table>
<thead>
<tr>
<th>NGL LOGSET Parameters</th>
<th>LOGSET attributes used by this group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logset Compression</td>
<td>LOW (HIGH, LOW, NO)</td>
</tr>
<tr>
<td>Logset time span</td>
<td>70 (nD, nH, nM)</td>
</tr>
<tr>
<td>Max log buffers</td>
<td>10 (2-20)</td>
</tr>
<tr>
<td>Max read buffers</td>
<td>4 (2-99)</td>
</tr>
<tr>
<td>Deferred write time</td>
<td>60 (1-999 sec.)</td>
</tr>
<tr>
<td>Minimum log file data sets (LDS)</td>
<td>2 (1-99)</td>
</tr>
<tr>
<td>Maximum log file data sets (LDS)</td>
<td>5 (1-99)</td>
</tr>
<tr>
<td>Space to allocate (per LDS)</td>
<td>100 (1-9999 MB) note: 1 CYL=720KB</td>
</tr>
<tr>
<td>LDS Allocation type</td>
<td>_______ (SMS, VOL, NONE)</td>
</tr>
<tr>
<td>LDS Volume</td>
<td>_______ (required for type=VOL)</td>
</tr>
<tr>
<td>LDS DFSMS Data class</td>
<td>_______ (required for type=SMS)</td>
</tr>
<tr>
<td>LDS DFSMS Management class</td>
<td>_______ (required for type=SMS)</td>
</tr>
</tbody>
</table>
BMC recommends using SMS values that have access to many volumes. If you specify a volume, BMC recommends that you specify a group name that would have access to a pack of volumes. If your SMS rules are set based on the HLQ in the DSN Prefix field, you should specify NONE for LDS Allocation Type and you do not need to fill in any of the LDS Volume or SMS fields.

9 If you plan to archive the trace data, review these fields:

- **Enable Archiving**: Y (Y=Yes, N=No)
- **Archive Wait Time**: 600 (1-9999 Sec)
- **Archive post processing job**: (optional) DOMPARM PDS member
- **Max days to keep archives**: 0 (1-999 Days, 0=NoLimit)
- **Max number archives to keep**: 0 (1-999 Data sets, 0=NoLimit)
- **Max combined size of archives**: 0 (1-999999 Mb, 0=NoLimit)
- **Archive file Allocation type**: (SMS, UNIT, VOL, NONE)
- **Archive Volume**: (required for type=VOL)
- **Archive Unit**: (required for type=UNIT)
- **Archive DFSMS Data class**: (required for type=SMS)
- **Archive DFSMS Management class**: (required for type=SMS)
- **Archive DFSMS Storage class**: (required for type=SMS)
- **Archive GDG**: N (Y=Yes, N=No)
- **Archive DSN prefix**: AFDQA.N11J.OBJ
- **Alternate full archive DSN**: 

10 Expand and review **Subsystems supported by this group** to ensure that the correct DB2s are listed for this Data Collector.

An asterisk (*) in this field indicate that all DB2 subsystems in the DB2 Monitor List that are active on the LPAR are monitored.

11 Press **F3** to save the option set.

### Verifying the product for data sharing members

This topic applies to APPTUNE, SQL Explorer, and SQL Performance.

Make sure that you define a DB2 subsystem in the DOMPLEX option set for every data sharing member in the data sharing groups.

See “Checking or modifying the DB2 subsystems to monitor” on page 251 to display a list of the DB2 subsystems defined to the DOMPLEX or to add a DB2 subsystem to the DOMPLEX.

The Installation System customizes a member in the install JCL for each DB2 subsystem. The member is called PSS2ssid, where ssid is the subsystem identifier. These members contain the DB2 libraries and the product plan name. For data sharing groups, verify that a PSS2ssid member has been replicated for each data sharing subsystem. If data sharing members are at different versions or modes of
DB2, BMC recommends that you use different plans and collection IDs for the members.

If your DB2 libraries are in the LINKLIST, leave the values blank for the DSNEXIT= and DSNLOAD= parameters in the PSS2ssid member.

**Customizing the CLISTs for SQL Explorer and CATALOG MANAGER**

This topic applies only to SQL Explorer and SQL Performance.

You can launch the common Explain component from CATALOG MANAGER, enabling you to access and analyze SQL from CATALOG MANAGER. You can also launch the SQLX edit macro of the SQL Explorer product from a TSO Edit session outside the product environment to Explain or execute a single SQL statement.

**Setting up the SQLX edit macro**

To use the SQLX edit macro, you must make some adjustments to your TSO data sets and libraries.

You can make these adjustments in one of the following ways:

- Concatenate a CLIST library containing the SQLX member with your logon procedure SYSPROC DD statement.
- Copy the SQLX member from your HLQ.UBBCLIB data set to a common CLIST library.

**Addition of subsystem information for the SQLX edit macro and the ACTPSS CLIST**

During the product installation, the SQLX edit macro and the ACTPSS CLIST are customized for information from the installation that is performed on each subsystem.

SQLX and ACTPSS are then copied into your product UBMCCCLIB library. You might need to customize these members for subsequent installations or for additional data sharing members. Skeleton members, #SQLX and ACTPSS, can be found in the product CLIB dataset, respectively, if no customization took place during installation. Copy the skeleton members to SQLX and ACTPSS in your CLIST or user library and customize them as described in this section.
Adding subsystem information after installation

To add subsystem information from subsequent installations to SQLX and ACTPSS after installation, append the subsystem information at the top of the member following the /* REXX line. The closing comment symbols (*/) must be on a line following the customized lines. For an example, see Figure 28 on page 236.

The format of the data is as follows where *ssid* is your subsystem identifier:

```
ssid keyword value
```

Table 105 on page 235 lists the keywords that you can specify, with a description of each keyword and an example for each value.

**Table 105: Keywords for adding subsystem information to SQLX and ACTPSS**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
<th>Sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLAN</td>
<td>SQL Explorer plan name</td>
<td>DAA vvrrD1 a</td>
</tr>
<tr>
<td>EXIT</td>
<td>DSNEXIT library for SSID</td>
<td>SYS3.DEAH.DSNEXIT</td>
</tr>
<tr>
<td>LOAD</td>
<td>DSNLOAD library for SSID</td>
<td>SYS2.DB2 vrrm.DSNLOAD</td>
</tr>
<tr>
<td>CNTL</td>
<td>Control library for SSID <em>(HLQ.LLQAMP)</em></td>
<td>BMCPERF.LLQAMP</td>
</tr>
<tr>
<td>MLIB</td>
<td>Message library for SSID <em>(HLQ.LLQMLIB)</em></td>
<td>BMCPERF.LLQMLIB</td>
</tr>
<tr>
<td>PLIB</td>
<td>Panel library for SSID <em>(HLQ.LLQPLIB)</em></td>
<td>BMCPERF.LLQPLIB</td>
</tr>
<tr>
<td>SLIB</td>
<td>Skeleton library for SSID <em>(HLQ.LLQSLIB)</em></td>
<td>BMCPERF.LLQSLIB</td>
</tr>
<tr>
<td>CLIB</td>
<td>CLIST library for SSID <em>(HLQ.LLQCLIB)</em></td>
<td>BMCPERF.LLQCLIB</td>
</tr>
<tr>
<td>LLIB</td>
<td>LOAD library for SSID <em>(HLQ.LLQLINK)</em></td>
<td>BMCPERF.LLQLINK</td>
</tr>
<tr>
<td>DLIB</td>
<td>LOAD library for DB2 common code <em>(HLQ.LLQLINK)</em></td>
<td>BMCPERF.LLQLINK</td>
</tr>
<tr>
<td>TLIB</td>
<td>ISPF table library for SSID <em>(HLQ.LLQTLIB)</em></td>
<td>BMCPERF.LLQTLIB</td>
</tr>
<tr>
<td>XLIB</td>
<td>LOAD library for infrastructure code <em>(HLQ.LLQLINK)</em></td>
<td>BMCPERF.LLQLINK</td>
</tr>
<tr>
<td>PSWD</td>
<td>Password data set <em>(HLQ.BMCPSWD)</em></td>
<td>BMCPERF.BMCPSWD</td>
</tr>
</tbody>
</table>

a vvrr is the version and release level for the current release.
Figure 28 on page 236 shows a complete example of this information for the subsystem ID DEAH.

Figure 28: Sample of appended subsystem information for subsystem ID DEAH

```
/* REXX ************************************************
DEAH PLAN DAAvvrD1
DEAH EXIT SYS3.DEAH.DSNEXIT
DEAH LOAD SYS2.DSNLOAD
DEAH CNTL BMCPERF.BMCSAMP
DEAH MLIB BMCPERF.BMCMLIB
DEAH PLIB BMCPERF.BMCPLIB
DEAH SLIB BMCPERF.BMCSSLIB
DEAH CLIB BMCPERF.BMCCLIB
DEAH LLIB BMCPERF.BMCLINK
DEAH DLIB BMCPERF.BMCLINK
DEAH TLIB BMCPERF.BMCTLIB
DEAH XLIB BMCPERF.BMCLINK
DEAH PSWD BMCPERF.BMCPSWD
*/
```

To append the subsystem information, begin entering data either on the second line of the comments section of the SQLX edit macro or between the /* REXXX line and the closing comment line (*/) of the ACTPSS CLIST. The data can begin in any column. Enter complete information for all SSIDs that you want to access.

Creating indexes to improve performance

This topic applies to APPTUNE, SQL Explorer, MainView for DB2—Data Collector, BMC System Performance, and SQL Performance. It does not apply to Pool Advisor when it is run as a stand-alone product.

To improve performance, BMC Software recommends that you create indexes on the DB2 catalog.

To create indexes on the DB2 catalog tables

1. Follow the instructions in BMIDB2XA in the HLQ.UBMCSAMP data set to create the indexes.

To create indexes on the user plan tables

If your plan tables have many rows from performing BIND with EXPLAIN(YES) operations, BMC Software recommends that you add indexes to your plan tables. The following procedure describes how to create indexes on the user plan tables.

1. Follow the instructions in the DAADB2IX member in the HLQ.LLQSAMP data set (PSSSAMP, BBSAMP, or your runtime SAMP data set) to create the indexes on your plan tables.
Generating Help text from DB2 trace record field descriptions

The Help job generates Help text from DB2 trace record field descriptions, which are located in the DSNWMSGS member of the DB2 SDSNIVPD data set. Run this job if you want to be able to retrieve DB2 field descriptions from DSNWMSGS while using the product. This task is optional, and applies to APPTUNE, Pool Advisor, MainView for DB2 - Data Collector, System Performance, and SQL Performance. It does not apply to SQL Explorer when it is run as a stand-alone product.

This task is optional, and applies to APPTUNE, Pool Advisor, MainView for DB2 - Data Collector, System Performance, and SQL Performance. It does not apply to SQL Explorer when it is run as a stand-alone product.

An example of a field and its description is as follows:

| OBSGET (number of getpages) |

To generate Help text from DSNWMSGS, modify and submit the JCL provided in the DOMHELP member of the LLQSAMP library (DOMSAMP, BBSAMP, or runtime SAMP data set). The DBC subsystem cannot be active while this job is running.

The Help job performs the following tasks:

- Converts DSNWMSGS macro text to loadable Help text records
- Copies the loadable Help text records to the HELP data set
- Reorganizes the HELP data set

For information about using the online Help facility, see the user guides for the products that you are installing.

Editing or reviewing the DBC JCL procedure

This task is required. The task does not apply to SQL Explorer or OPERTUNE. To use the DBC component, you must configure the DBC started task.
Before you begin

Review this information before modifying the DBC JCL procedure (DBC$STC). Figure 29 on page 238 shows an example of the DBC$STC job generated by the Installation System.

Figure 29: DBC$STC JCL

```
//DBC    PROC  ACC=,  
//             SSID=DC01,       ===> SSID
//             G=DCPLEX,        ===> GROUP
//             T=NO,           ===> TRACE
//             TIM=1440        ===> 
//*
//*********************************************************************
//*
//* DESCRIPTION:
//*   BMC SOFTWARE DBC SUBSYSTEM STARTUP JCL PROCEDURE.
//*
//* REQUIRED DD STATEMENTS:
//*   DBCPARMS - DBC SUBSYSTEM INITIALIZATION PARAMETERS
//*   DBCPRINT - DBC SUBSYSTEM MESSAGES
//*
//* OPTIONAL DD STATEMENTS:
//*   STEPLIB  - OPTIONAL ONLY IF THE DBC LOAD LIBRARY IS IN THE SYSTEM
//*             LINK LIST.
//*   DBCSECUR - DBC SUBSYSTEM SECURITY OPTIONS
//*   SYSPRINT - RECOMMENDED WITH RECFM=VA
//*
//*
//* CUSTOMIZATION STEPS:
//*   - COPY THIS PROC TO YOUR SYSTEM PROCLIB
//*   - APF AUTHORIZE THE DBC STEPLIB DATA SET(S).
//*   - START THE DBC ADDRESS SPACE.  FOR EXAMPLE:
//*     /S DBC$STC
//*
//* NOTES:
//*   THE DBC SUBSYSTEM IS A LONG-RUNNING-SERVICE ADDRESS SPACE THAT
//*   NORMALLY REMAINS ACTIVE FOR THE LIFE OF AN IPL.  THEREFORE, BMC
//*   DOES NOT RECOMMEND STARTING THE DBC SUBSYSTEM AS A BATCH JOB.
//*   DOING SO CAUSES THE JES INITIATOR TO BE BUSY FOR THE LIFE OF
//*   THE DBC SUBSYSTEM.  IF YOU WANT TO RUN THE DBC AS A BATCH
//*   JOB, REPLACE THE PROC STATEMENT WITH A VALID JCL JOB CARD.
//*
//*********************************************************************
//DBC     EXEC PGM=DBCMAIN,REGION=0M,ACCT=&ACC,TIME=&TIM,
//        PARM='SSID=&SSID,GROUP=&G,TRACE=&T'
//STEPLIB   DD DSN=BMCPERF.BMCLINK,
//             DISP=SHR
//BMCPWD   DD DISP=SHR,
//          DSN=BMCPERF.BMCPWD
//DBCPRINT DD SYSOUT=*,RECFM=VA
//SYSPRINT DD SYSOUT=*,RECFM=VA
//SYSTEM   DD SYSOUT=*,RECFM=VA
//DBCPARMS DD DISP=SHR,
//          DSN=BMCPERF.BMCSAMP($DBC&SSID)
//DBCSECUR DD DISP=SHR,
//          DSN=BMCPERF.BMCSAMP($SEC&SSID)
//REGISTRY DD DISP=SHR,
//          DSN=BMCPERF.DC01.REGISTRY
//DOMTMPLT DD DISP=SHR,
//          DSN=BMCPERF.DC01.TEMPLATE
//DOMPARMS DD DISP=SHR,
//          DSN=BMCPERF.BMCPARM
```
WARNING

BMC Software recommends that you note the following restrictions before making changes to the STEPLIB statement in the DBC PROC. The load libraries that are specified in the STEPLIB statement must be APF authorized. If you have one runtime or deployment data set, you can reference only that data set on the STEPLIB line.

When the product PROC is invoked, the SSID parameter identifies the SSID of the DBC subsystem. The GROUP parameter specifies the DBC group to which this DBC subsystem belongs. For more information about the DBC started task, see BMC Infrastructure Components Administration Guide.

To edit or review the JCL procedures for the DBC (all products)

1. Locate and review the DBC started task procedure.

2. Start the DBC (which runs as a z/OS subsystem) by using one of the following methods:
   - By issuing the z/OS START command from an operator console
   - By using a batch job

To start the DBC subsystem by using the z/OS START command for the product PROC

1. Copy the modified PROC into your SYS1.PROCLIB (or equivalent) started task library.

2. Ensure that you have performed all security authorization steps.

   For authorization requirements, see the Installation System documentation. The procedure for defining an AUTHID for a started task varies with the security system used.

3. Issue the START command.

To start the DBC subsystem by using a batch job

WARNING

BMC Software recommends executing the products in batch only when testing the initial installation. After initial installation, run the product as a started task. Stopping the product when it is running in batch abnormally terminates the initiator in which it was running.

1. Edit a data set to submit the DBC subsystem JCL.
2 Create a JOB statement that meets your site requirements.

3 Copy the modified PROC JCL into the data set after the JOB statement.

4 Append the following statement to the PROC JCL (where ssid is the DBC subsystem):

```plaintext
// PEND
// EXEC PROC=DOMssid
```

The following example starts DBC subsystem DC01.

```plaintext
// MONITOR EXEC PROC=DOMPROC,SYS=DC01.
```

5 Press F3 to save the data set.

**Where to go from here**

DOMPLEX option sets are created by using the **Administration** function. For instructions for reviewing the DOMPLEX option set, see “Verifying or customizing the DOMPLEX option set” on page 247.

The dispatching priority of the DBC subsystem should be higher than that of the DB2 MSTR address spaces to be monitored and should be lower than the IRLM.

**Adding or replacing the CLIST member for the ISPF interface**

This step is **required**. You can add or replace the CLIST for the ISPF interface.

1 This task varies, depending on whether you used the Installation System to modify and submit the JCL:

   - If you used the Installation System to modify and submit the JCL (tailored model), replace the DOMCLIST member that executes the product initialization in your CLIST library with the member from the JCL library.

   - If you did not use the Installation System to modify and submit the JCL, use the DOMCLIST member in the BBCLIB library (untailored model), and follow the modification instructions provided to point to the new product libraries. Modify this CLIST to specify the new product data set names. This CLIST dynamically allocates ISPF libraries and invokes the product.

2 Execute the CLIST by issuing the command **EX DOMCLIST**.
If your site uses VB CLISTs rather than FB CLISTs, you can reblock the CLIST by executing DOMRBLK provided in the DOMSAMP, BBSAMP, or runtime SAMP data set. Execution of DOMRBLK allocates a new VB CLIST. As a result, you must modify DOMRBLK to provide old and new high-level qualifiers for data sets and a volume for the allocation of the new CLIST library.

Figure 30 on page 241 shows the CLIST for executing a product.

**Figure 30: CLIST for executing a product**

```clist
PROC 0 PRD() +
   P() +
   SSID() +
**********************************************************************/
/*                        BMC CHANGE NOTES :                        */
/*                                                                   */
/*     $ MCCHG BQ26349,MAC COMMENT ON DP= PARM               @301850 */
/*                                                                   */
/**********************************************************************
/*    CLIST FOR EXECUTION OF THE SYSTEM AND SQL PERFORMANCE PRODUCTS */
/*                                                                   */
/*    THE PRD= PARM CAN BE USED TO CONTROL THE EXECUTION OF WHICH     */
/*    LICENSED SYSTEM AND SQL PERFORMANCE PRODUCTS WILL BE SHOWN AS   */
/*    OPTIONS ON THE INITIAL PRODUCT MENU.                          */
/*    THE 'PRD' PARM IS ALSO USED TO CONTROL THE ALLOCATION OF       */
/*    ADDITIONAL FILES REQUIRED BY SOME COMPONENTS. THE COMPONENT     */
/*    CODES ARE AS FOLLOWS:                                          */
/*    PRD(A)   ACTIVITY MONITOR FOR DB2 (LEGACY ONLY)               */
/*    B      MAINVIEW FOR DB2                                       */
/*    P      POOL ADVISOR                                          */
/*    O      OPERTUNE                                              */
/*    D      BMC SYSTEM PERFORMANCE SOLUTION (INCLUDES B,P,O)        */
/*    Q      BMC APPTUNE                                           */
/*    S      BMC SQL EXPLORER                                       */
/*    I      BMC SQL PERFORMANCE FOR DB2 (INCLUDES Q,S)              */
/*    TO SPECIFY MULTIPLE PRODUCTS, USE ALL COMPONENT CODES TOGETHER.*/
/*    FOR EXAMPLE: 'P(PRD=PQS)'                                     */
/*    SPECIFYING 'PRD()' WILL CAUSE ALL FILE TYPES TO BE ALLOCATED   */
/*    IF THEY EXIST.                                                */
/*    THE DP= PARM CAN BE USED TO SPECIFY A DEFAULT DOMPLEX THAT WILL*/
/*    BE AUTOMATICALLY SELECTED FOR USE DURING YOUR PRODUCT SESSION.*/
/*    THE DATA COLLECTOR FOR THAT DOMPLEX MUST BE ONE YOU ARE        */
/*    AUTHORIZED TO USE. FOR EXAMPLE: P(DP=DOMPLEX)                 */
/*    TO SPECIFY BOTH PARM (PRD AND DP), YOU MUST SEPARATE THE PARM S*/
/*    WITH A COMMA AND ENCLOSE THE PARM S IN SINGLE QUOTES.         */
/*    FOR EXAMPLE: P('PRD=P0,DP=DOMPLEX') SSID()                   */
/*    THE 'SSID' PARM IS USED TO PASS THE SUBSYSTEM IDENTIFIER FROM   */
/*    THE BMCDB2PR PANEL TO THE SQL EXPLORER MAIN MENU.              */
/**********************************************************************
CONTROL MSG NOSYMLIST NOCONLIST NOLIST NOFLUSH
```

Post-installation tasks
IF &SYSISPF = ACTIVE THEN DO
WRITE THIS CLIST REQUIRES ISPF TO BE ACTIVE
EXIT CODE(12)
END
SET &PRDLEN = &LENGTH(&PRD)
IF &PRDLEN GT 0 THEN +
    SET &P = &STR(PRDR=A0PRD,&P)
ALLOC F(DOMPLIB) +
    DA('BMCPERF.BMCPLIB') SHR REU
ALLOC F(DOMTLIB) +
    DA('BMCPERF.BMCTLIB') SHR REU
ALLOC F(DOMLOAD) +
    DA('BMCPERF.BMCLINK') SHR REU
ALLOC F(BMCPWD) +
    DA('BMCPERF.BMCPSWD') SHR REU
ALLOC F(DOMCUST) +
    DA('BMCPERF.BMCCSTM') SHR REU
ALLOC F(DOMBARC) +
    DA('BMCPERF.COPYDIR') SHR REU
ALLOC F(DOMPREF) +
    DA('BMCPERF.PROFILE') SHR REU
ALLOC F(DOMAUTH) +
    DA('BMCPERF.SECURITY') SHR REU
ALLOC F(DOMHELP) +
    DA('BMCPERF.HELP') SHR REU
/* SPECIAL PSS ALLOCATIONS
***********************************************************************************/
PSSALLOC: +
ALLOC F(PSSMLIB) +
    DA('BMCPERF.BMCMLIB') SHR REU
ALLOC F(PSSSLIB) +
    DA('BMCPERF.BMCSSLIB') SHR REU
ALLOC F(PSSCLIB) +
    DA('BMCPERF.BMCCLIB') SHR REU
ALLOC F(PSSCNTL) +
    DA('BMCPERF.BMCSAMP') SHR REU
ISPEXEC LIBDEF ISPMLIB LIBRARY ID(PSSMLIB)
ISPEXEC LIBDEF ISPSLIB LIBRARY ID(PSSSLIB)
ALTLIB ACTIVATE APPLICATION(CLIST) FILE(PSSCLIB) UNCOND
PSSSKIP: CONTROL MSG
/* REMOVE COMMENT ON SYSOUT ALLOCATION IF SORT MESSMAGES ARE BEING
* SENT TO THE TERMINAL.
* REMOVE COMMENT ON SORT WORK FILE ALLOCATIONS AND FREE STATEMENT
* AT THE END OF THIS CLIST TO PRE-ALLOCATE SORT WORK FILES.
***********************************************************************************/
/* ALLOC F(SYSOUT) DUMMY SHR REU
/* ALLOC F(U00OWK01) UNIT(SYSALLDA) SPACE(10,5) CYL NEW REU
/* ALLOC F(U00OWK02) UNIT(SYSALLDA) SPACE(10,5) CYL NEW REU
/* ALLOC F(U00OWK03) UNIT(SYSALLDA) SPACE(10,5) CYL NEW REU
/* ALLOC F(U00OWK04) UNIT(SYSALLDA) SPACE(10,5) CYL NEW REU
/* ALLOC F(U00OWK05) UNIT(SYSALLDA) SPACE(10,5) CYL NEW REU
/* ALLOC F(U00OWK06) UNIT(SYSALLDA) SPACE(10,5) CYL NEW REU
ISPEXEC LIBDEF ISPMLIB LIBRARY ID(DOMPLIB)
ISPEXEC LIBDEF ISPTLIB LIBRARY ID(DOMTLIB)
ISPEXEC LIBDEF ISPLLIB LIBRARY ID(DOMLOAD)
CONTROL NOMSG
FREE FI(SYSIN SYSPRINT)
CONTROL MSG
SET &PVSSID = &SSID
ISPEXEC VPUT (PVSSID) PROFILE
ISPEXEC SELECT CMD(DOMDMAIN &P) MODE(FSCR) NEWAPPL(DOM2) PASSLIB
ISPEXEC LIBDEF ISPLLIB
ISPEXEC LIBDEF ISPPLIB
ISPEXEC LIBDEF ISPTLIB
ISPEXEC LIBDEF ISPMLIB
Making products available from a menu

You can make products available from the menu. This task is optional.

To make products available from an ISPF menu

Modify ISR@PRIM or an equivalent panel as follows:

1. In the )BODY area, add the following line:
   ```
   %O      + SYSTEM AND SQL PERFORMANCE PRODUCTS FOR DB2+
   ```

2. In the )PROC area, add the following line:
   ```
   O,'CMD(DOMCLIST) NEWAPPL'
   ```

To make products available from the panel customized by the installation

Modify ISR@PRIM or an equivalent panel as follows:

1. In the panel area, add the following line:
   ```
   %P     + SYSTEM AND SQL PERFORMANCE PRODUCTS FOR DB2
   ```

2. In the )PROC area, add the following line:
   ```
   P,'PANEL(BMCDISPN)'
   ```

3. Exit and reenter ISPF.

4. Invoke the products by selecting option P from the System and SQL Performance products Install System menu or a panel of your choice.
Note
If your system security restricts the access of command processors under TSO, you must add DOMDMAIN, DMDQIED2, PSSQLX, PSSCATI, LGCOMAIN, and PSSDCL (for SQL Explorer) to the list of commands that are allowed.

Installing maintenance has no effect on product authorization. However, you must ensure that your product authorization tables reside in the new production libraries. For more information, see the Installation System documentation.

Invoking SQL Explorer directly

This task is optional.

To invoke the SQL Explorer for DB2 product directly, use the PSSCLIST that was customized during installation.

Invoking System and SQL Performance products without LIBDEFS

DOMCLIST uses the ISPF LIBDEF command to allocate all BMC Software product libraries. The installation system customizes DOMCLIST to include the data set names that you used when you installed the products. Subsequent LIBDEF commands from within the product are stacked. This task is optional.

For those BMC Software products that provide an online dialog, the installation system generates an ISPF interface, based on the options and products that you specify during installation. BMC Software products that are installed with different high-level qualifiers (that is, products that are installed individually and that might reside in different libraries) can be accessed from the interface.

The interface consists of a CLIST (BMCDRIVC) and a panel (BMCDRIV) that lists all of the products that you installed. CLISTs that are specific to the individual products in this list are invoked when you select them. The System and SQL Performance products use DOMCLIST. You can use this combination without making changes to your TSO logon procedure. BMC Software recommends that new users use the ISPF interface that BMC provides. The System and SQL Performance products require that you execute the CLIST from one of the ISPF dialog panels in your system.
Before you begin

If you have your own ISPF environment and do not want to invoke DOMCLIST with the LIBDEF command, be sure to include the DOMCLIST-referenced data sets in your environment.

To invoke BMC products without LIBDEFs

1. Allocate the following DDs:
   - DOMLOAD (for the product load libraries)
   - PSSCNTL (for the sample data set that contains the default layout member for Explain, Workload Access Path Compare, and Index Advisor processing) and PSS2 ssid members.
   - BMCPSWD (for the password data set)

2. Perform an ALTLIB command on the PSSCLIB file for the product CLIST library.

3. Invoke the product.

   Execute the following command from your panel, where *pp* is a list of the products to enable and *dcOptionSetName* is the DOMPLEX option set:

   ```
   SET P = &STR('PRD=pp,DP=dcOptionSetName')
   ISPEXEC SELECT CMD(DOMDMAIN &P) MODE(FSCR) NEWAPPL(DOM2) PASSLIB
   ```

You can enable as many of the following products as needed:

<table>
<thead>
<tr>
<th>Option</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>MainView for DB2—Data Collector</td>
</tr>
<tr>
<td>P</td>
<td>Pool Advisor for DB2</td>
</tr>
<tr>
<td>O</td>
<td>OPERTUNE for DB2</td>
</tr>
<tr>
<td>D</td>
<td>BMC System Performance for DB2 (includes B, P, and O)</td>
</tr>
<tr>
<td>Q</td>
<td>APPTUNE for DB2</td>
</tr>
<tr>
<td>S</td>
<td>SQL Explorer for DB2</td>
</tr>
<tr>
<td>I</td>
<td>BMC System Performance for DB2 (includes Q and S)</td>
</tr>
</tbody>
</table>
Verifying or changing the global resource enqueues

This task is required for shared-DASD environments that use a global resource manager like GRS or MIM.

Ensure that SYSTEMS-level enqueues are propagated throughout the complex. The System and SQL Performance products mostly use SYSTEMS enqueues with resource names that are prefixed by AMFORDB2, BMCDBCR, and BMCLGC.

Contact BMC Support to allow RNL overrides.

Refreshing the MVS Linklist Lookaside

This task is optional. Refresh the LINKLST data set only if both of the following conditions are true:

- You are using the MVS Linklist Lookaside (LLA) feature.
- You have installed the product load modules into a LINKLST data set.

In a shared-DASD environment, refresh the LINKLST data set on each CPU that is using one or more of the System and SQL Performance products.

Verifying the product authorization

All BMC Software products require product authorization before you can use them. This section describes how you can authorize your products.

You can apply your BMC Software authorization passwords when you install the System and SQL Performance products. If you are a licensed user and have already received and applied the permanent BMC Software authorization passwords, ensure that you save the appropriate authorization modules and copy them to the new load library after you execute the Full installation. The authorization modules are created when the password is added.

You can also use the BMC Software Product Authorization utility to apply passwords and to change your CPU configuration. To use the Product Authorization utility, see the chapter on applying product passwords in the Installation System documentation.
This section describes how to start the System and SQL Performance products that you have installed, create or review profiles, and check key values to make them consistent with the standards at your site.

Nota Not all customization tasks apply to all System and SQL Performance products. In some cases, the panels that are encountered and the fields that are displayed on product panels differ, depending on the active product mix. The panel examples in this book assume that all System and SQL Performance products are installed and active. Information that is specific to one or more products is identified in the text.

The following list summarizes the System and SQL Performance products customization tasks.

- “Verifying or customizing the DOMPLEX option set” on page 247
- “Verifying or changing DOMPLEX parameters” on page 262
- “Checking the default User Profile” on page 266

Nota Before you start to customize the System and SQL Performance products, perform the following tasks:

- APF authorize the load library data sets.
- If you are using RACF add your product user ID to table ICHRIN03.

Verifying or customizing the DOMPLEX option set

This task is required for full and SSID installations. This task is not required if you are installing only SQL Explorer or OPERTUNE.

DOMPLEX option sets define one or more Data Collectors for monitoring DB2. The Data Collectors run as DOM agents with the DBC subsystem.

A DBC subsystem in a DOMPLEX can monitor all of the DB2 subsystems on the same z/OS image. BMC recommends that each DBC subsystem in the DOMPLEX share the same VSAM data sets (for more information, see “MVS security” on page 106) and product load libraries. You can define multiple DOMPLEXes, but each DBC subsystem can be defined to only one DOMPLEX.

The DOMPLEX option set contains the parameters that affect product initialization, identifies and defines the DB2 subsystems to be monitored, and defines log files. You
can modify these values as you follow the examples in this chapter. These examples use a DOMPLEX option set called DC01PLEX and a Data Collector called DC01.

Data Collector names must consist of four characters and cannot be the same as the name of the DB2 subsystem or any other subsystem on the z/OS system. The Data Collector name should match the name of the DBC subsystem ID.

This task consists of the following subtasks:

- “Starting a product session” on page 248
- “Checking the values in the DOMPLEX option set” on page 249
- “Checking or modifying the DB2 subsystems to monitor” on page 251
- “Checking or modifying the output groups” on page 254

### Starting a product session

You do not need an active Data Collector to access the Report Manager, but functionality will be limited to those tasks that do not require an active Data Collector. Some Administration functions require that the DBC started task be active and that the DB2 Product Configuration agent is running.

**To start a product session**

1. Log on to TSO.
2. Invoke ISPF from TSO.
3. Navigate to the ISPF menu that you previously modified to invoke the System and SQL Performance products (see “Adding or replacing the CLIST member for the ISPF interface” on page 240).
4. Select the option to invoke the products or execute your CLIST.

The product logo is displayed, followed by a main menu.

---

**Note**

The main menu that is displayed reflects the active product mix. If a single product is invoked, the main menu for that product is displayed. If you are invoking multiple System and SQL Performance products or solutions, a common main menu listing those products and solutions is displayed (see Figure 31 on page 248). Only active products are listed on the menu.

---

**Figure 31: System and SQL Performance for DB2 main menu**

<table>
<thead>
<tr>
<th>Command</th>
<th>System and SQL Performance for DB2</th>
<th>18:17:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Data Collector</td>
<td>A62D</td>
<td>Status</td>
</tr>
</tbody>
</table>

248  *BMC Products and Solutions for DB2 Customization Guide*
Checking the values in the DOMPLEX option set

You can view the DOMPLEX option set within the interface.

1. Display the Administration menu (Figure 32 on page 249).

   The Administration option appears on all main menus, but the option number is not the same on all main menus. Select the option that is labeled Administration.

   **Figure 32: Administration menu**

<table>
<thead>
<tr>
<th>Command</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. USER PROFILES</td>
<td>VIEW/MODIFY USER PROFILES</td>
</tr>
<tr>
<td>2. DOMPLEX OPTION SETS</td>
<td>VIEW/MODIFY DOMPLEX OPTION SETS</td>
</tr>
<tr>
<td>3. MAINTENANCE</td>
<td>VIEW MAINTENANCE APPLIED SINCE INSTALL</td>
</tr>
<tr>
<td>4. APPTUNE FILTERS</td>
<td>VIEW/MODIFY APPTUNE FILTER OPTION SETS</td>
</tr>
</tbody>
</table>

2. From the Administration menu, select option 2 (DOMPLEX Option Sets) and press Enter.

   The DOMPLEX Options Set panel (Figure 33 on page 249) is displayed.

   **Figure 33: DOMPLEX Option Sets panel**

   | IDOMPLEX | Canned DOMPLEX optionset | yyyy/10/02 13:28:20 RDADAC4 |
   | AFDPLEX | AFD DOMPLEX | yyyy/11/02 10:23:33 RDHPSH1 |
   | AFDOA9BC | AFOQA 10.1 PLEX FOR DBC/NGL | yyyy/11/02 10:23:38 RDHPSH1 |

3. From the DOMPLEX Option Sets panel, select the DOMPLEX option set that you created during installation.

   This panel is also the starting point for creating a new DOMPLEX option set.
To select a DOMPLEX option set for modification, move the cursor to the field beside that DOMPLEX, type E (edit), and press Enter.

To create a new DOMPLEX option set, type I next to the product or solution name and press Enter.

To create a new DOMPLEX option set by copying from an existing option set, type C in the field next to the name of the option set to be copied and press Enter.

The DOMPLEX option set panel (Figure 34 on page 250) is displayed.

**Figure 34: DOMPLEX option set panel**

<table>
<thead>
<tr>
<th>Command ====&gt;</th>
<th>DC01PLEX - Test Option Set</th>
<th>Scroll ===&gt; PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter: Off</td>
<td>Parameters that apply to entire DOMPLEX</td>
<td></td>
</tr>
<tr>
<td>+ DOMPLEX Parameters</td>
<td>Data Collector(DBC) subsystems in DOMPLEX</td>
<td></td>
</tr>
<tr>
<td>+ Data Collector List (1)</td>
<td>DB2 Sub-systems to be monitored</td>
<td></td>
</tr>
<tr>
<td>+ DB2 Monitor List (11)</td>
<td>Output Groups - valid range: 001-256</td>
<td></td>
</tr>
<tr>
<td>+ OutGp DCID DspSize (6)</td>
<td>End of List ***********************</td>
<td></td>
</tr>
</tbody>
</table>

The DOMPLEX option set panel allows you to specify the options for an individual option set. This panel contains the following sections:

- Use the **DOMPLEX Parameters** section to set values that apply to the entire DOMPLEX.

- Use the **Data Collector List** section to define the initialization parameters for each Data Collector (for example, the number of concurrent batch and online users allowed).

- Use the **DB2 Monitor List** section to identify and define the DB2 subsystems that can be monitored by the Data Collectors in the DOMPLEX.

- Use the **OutGp DCID DspSize** section to define the output groups that are used to buffer trace records and to define and allocate log files where records are written from the output groups.

For ease of installation, this book assumes that default options are used during installation for most parameters and discusses only the **DB2 Monitor List** and **OutGp DCID DspSize** sections.

A detailed description of all DOMPLEX option set values is provided in the *System and SQL Performance for DB2 Administrator Guide* and in the online Help that accompanies the products.

If you press F1 while the cursor is positioned on an input or output field on a panel, specific information about that field is displayed. To view general
information or information about a panel, use the Help menu at the top of the panel.

**Checking or modifying the DB2 subsystems to monitor**

One Data Collector can monitor all DB2 subsystems on the z/OS system.

*Note*

You must define at least one DB2 subsystem for each DOMPLEX option set. The Data Collector (DOM Agent) will not start unless there is at least one DB2 subsystem defined.

**To check or modify the DB2 subsystems to monitor**

1. At the DOMPLEX option sets panel, expand the DB2 Monitor List section.

   The DB2 subsystems that were specified during installation are listed in the Data Collector List section. You can delete DB2 subsystems from or add DB2 subsystems to the list that will be monitored by this DOMPLEX.

2. To add a DB2 subsystem, type **I** over the - sign next to **Data Collector List** and press **Enter**.

3. Type over the DB2 subsystem identifier with the value that you need to add.

   *Note*

   Use an asterisk (*) to specify all DB2 subsystems. If you use an asterisk, the definitions of all DB2 subsystems on the system will be the same.

4. Expand the DB2 subsystem for which you want to specify parameters, as shown in Figure 35 on page 251.

**Figure 35: DOMPLEX object set - Expanded DB2 Monitor List**

<table>
<thead>
<tr>
<th>File</th>
<th>Filter</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DCO1PLEX - Test Option Set</td>
</tr>
<tr>
<td>Scroll</td>
<td>PAGE</td>
<td></td>
</tr>
<tr>
<td>Command ====&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filters: Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+ DOMPLEX Parameters</td>
<td>Parameters that apply to entire DOMPLEX</td>
<td></td>
</tr>
<tr>
<td>- Data Collector List</td>
<td>Data Collector(DB) subsystem SSIDs in DOMP</td>
<td></td>
</tr>
<tr>
<td>Filter: Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- DB2 Monitor List (11)</td>
<td>DB2 Sub-systems to be monitored</td>
<td></td>
</tr>
<tr>
<td>- AFDA</td>
<td>DB2 SSID</td>
<td></td>
</tr>
<tr>
<td>Is this a production DB2? . . . . . . : N</td>
<td>(Y=Yes,N=No)</td>
<td></td>
</tr>
<tr>
<td>Monitor with MAINVIEW for DB2 - DC . . : N</td>
<td>(Y=Yes,N=No)</td>
<td></td>
</tr>
<tr>
<td>Monitor with Pool Advisor/System Perf.: N</td>
<td>(Y=Yes,N=No)</td>
<td></td>
</tr>
<tr>
<td>Monitor with APPTUNE . . . . . . . : N</td>
<td>(Y=Yes,N=No)</td>
<td></td>
</tr>
<tr>
<td>Dynamic Explain plan name. . . . . . . : DAA111D1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; DB2 IFCID to be traced automatically</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; DB2 IFCID to be discarded</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&gt; BMC IFCID to be discarded</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class 2-In-DB2 elapsed timing info. . . : N</td>
<td>(Y=Yes,N=No)</td>
<td></td>
</tr>
<tr>
<td>Class 3-DB2 suspend timing info . . . . : N</td>
<td>(Y=Yes,N=No)</td>
<td></td>
</tr>
<tr>
<td>Class 5-Time spent doing IFI requests: N</td>
<td>(Y=Yes,N=No)</td>
<td></td>
</tr>
</tbody>
</table>

Chapter 7  Customizing System and SQL Performance  251
5 Check or set the values that define the DB2 subsystem, as described in Table 106 on page 252.

Table 106: DB2 Monitor List fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2 SSID</td>
<td>Specify the subsystem ID of the DB2 being defined.</td>
</tr>
<tr>
<td>Is this a production DB2?</td>
<td>Specify whether this is a production DB2. Valid values are Y and N.</td>
</tr>
</tbody>
</table>

**Monitor with MainView for DB2 - DC**

Specify whether MainView for DB2 Data Collector should automatically monitor this DB2 subsystem when its associated Data Collector is started. Valid values are:

- **Y**—the Data Collector automatically starts traces at collector initialization
- **N**—the Data Collector does not automatically start traces

**Note:** Specifying Y prevents interruptions to Data Collector processing by other products that use the Data Collector common codes (such as APPTUNE).

**Monitor with Pool Advisor/ System Perf**

Specify whether Pool Advisor should automatically monitor this DB2 subsystem when its associated Data Collector is started. Valid values are:

- **Y**—Pool Advisor automatically starts traces at collector initialization
- **N**—Pool Advisor does not automatically start traces

**Note:** Specifying Y prevents interruptions to Data Collector processing by other products that use the Data Collector common codes (such as APPTUNE).

**Monitor with APPTUNE**

Specify whether to collect data automatically for APPTUNE reporting at Data Collector initialization. Valid values are:

- **Y**—collect data from this DB2 for APPTUNE reporting
- **N**—do not collect data from this DB2 for APPTUNE.

**Note:** This field applies only to APPTUNE and SQL Performance for DB2.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Explain plan name</td>
<td>Specify the name of the plan used by DB2 for Dynamic Explain. This value must be the same as the plan name bound on this DB2 subsystem during installation. The default plan name in the installation JCL is DAA ( vvrD1 ) where ( vvr ) is the current release level of the product. If this default is used at installation, you must specify DAA ( vvrD1 ) here. If you used a different name at installation, you must specify that name here. <strong>Note:</strong> Pool Advisor does not use a plan.</td>
</tr>
<tr>
<td>(MainView for DB2 only) DB2 IFCIDs to be traced automatically</td>
<td>Use this option to select specific IFCIDs to trace. When you select this option, a new panel opens where you can specify the IFCIDs to be automatically traced. Separate values with a comma. You can enter a range of values by placing a hyphen between the first and last values.</td>
</tr>
<tr>
<td>(MainView for DB2 only) DB2 IFCIDs to be discarded</td>
<td>Use this option to prevent tracing of specific DB2 IFCIDs. When you select this option, a new panel opens where you can specify the specific DB2 IFCIDs that you do not want to trace. Separate values with a comma. You can enter a range of values by placing a hyphen between the first and last values.</td>
</tr>
<tr>
<td>(MainView for DB2 only) BMC IFCIDs to be discarded</td>
<td>Use this option to prevent tracing of specific BMC IFCIDs. When you select this option, a new panel opens where you can specify the specific BMC IFCIDs that you do not want to trace. Separate values with a comma. You can enter a range of values by placing a hyphen between the first and last values.</td>
</tr>
<tr>
<td>(MainView for DB2 only) Class2-In-DB2 elapsed timing info</td>
<td>Specify whether to collect Class 2-In-DB2 elapsed timing information. Valid values are Y and N.</td>
</tr>
<tr>
<td>(MainView for DB2 only) Class3-DB2 suspend timing info</td>
<td>Specify whether to collect Class 3-DB2 suspend timing information. Valid values are Y and N.</td>
</tr>
<tr>
<td>(MainView for DB2 only) Class5-Time spent doing IFI requests</td>
<td>Specify whether to collect Class 5-Time spent doing IFI requests. Valid values are Y and N.</td>
</tr>
<tr>
<td>(MainView for DB2 only) Class7-DB2 events (packages, DBRMs)</td>
<td>Specify whether to collect Class 7-DB2 events (packages, DBRMs). Valid values are Y and N.</td>
</tr>
<tr>
<td>(MainView for DB2 only) Class8-Wait time for packages</td>
<td>Specify whether to collect Class 8-Wait time for packages. Valid values are Y and N.</td>
</tr>
<tr>
<td>(MainView for DB2 only) Class 10-Optional package detail data</td>
<td>Specify whether to collect Class 10-Optional package detail data. Valid values are Y and N.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Collect dynamic SQL stats in stmt cache</td>
<td>Specify whether to collect dynamic SQL statistics in statement cache. Valid values are Y and N.</td>
</tr>
<tr>
<td>Collect static SQL stats in stmt cache</td>
<td>Specify whether to collect static SQL statistics in statement cache. Valid values are Y and N.</td>
</tr>
<tr>
<td>SQL Performance/APPTUNE options</td>
<td>Expand the SQL Performance/APPTUNE options group to specify the following values:</td>
</tr>
<tr>
<td>■ APPTUNE Filter Name</td>
<td>Specify the APPTUNE filter name to use. This name should match the name of the filter option set. Default filters are available. For more information about filter option sets, see the <em>System and SQL Performance for DB2 Administrator Guide</em>.</td>
</tr>
<tr>
<td>■ Fixed Collection Interval</td>
<td>Specify the interval (in minutes) at which data is written from the reduction table to the trace data sets. You can specify a value here and all intervals will have the same specified length. Specify 0 (zero) to set an individual Hourly Collection Intervals Schedule.</td>
</tr>
<tr>
<td>■ Hourly Collection Intervals Schedule (0-23)</td>
<td>Type Y at each hour boundary upon which an interval is to begin.</td>
</tr>
</tbody>
</table>

**Note:** BMC recommends that you specify the same statistical interval for all DB2s that are monitored by the same Data Collector. Valid values are any number in the range 1-1440.

---

6 Press F3 to save your values and return to the DOMPLEX Option Sets panel.

7 If prompted, enter the name of the option set and a description.

### Checking or modifying the output groups

An output group is a collection of specifications that is used to collect and process data for writing to the LOGSET log file data sets for batch or historical reporting.

#### To check or modify the output group

1 Select the Administration option from your product main menu.
2 On the Administration menu, select 2 (DOMPLEX Option Sets).

3 On the DOMPLEX Option Sets panel, type E next to the option set for which you want to modify option groups and press Enter.

4 Expand the Output Groups section on the DOMPLEX option set panel (as shown in Figure 36 on page 255).

**Figure 36: DOMPLEX option set panel - Expanded Output Group**

5 Expand the group number that you want to edit.

**Note**

If you need to create a new output group, type I on the - (minus) sign on the Output Groups section and press Enter.

The new output group is created at the top of the list with the number 001. If the group number 001 is already in use, rename the group by typing a new unused value in the range 001-256 over the 001 group number and pressing Enter.

6 Specify the following values:

a In the Group Number field, specify the number of the corresponding output group. Possible values are numbers in the range 001-256. In the Data Collector SSID field, specify the ID of the Data Collector that owns the output group.

Only the data from DB2s that are running on the same system as that Data Collector are captured and stored by this output group. If you specify DB2s that are running on a different system, they are ignored.

b In the Data space size, specify the size of the data space (in megabytes) assigned to collect and process the data for this output group before it is written to the log files.
Possible values are any number in the range 0-2000. The total amount of data space specified for all output groups defined to the same Data Collector cannot exceed 2 GB.

7 Specify the IFCIDs that you want to capture and store in this output group:

a Expand the Data Classes section.

b Specify the values for the parameters shown in Table 107 on page 256. The valid values for each parameter are Y (Yes) or N (No).

### Table 107: Data classes for an output group

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Related IFCIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>APERRO</td>
<td>Specify whether to collect APPTUNE error data.</td>
<td>APPTUNE/SQL Performance BMC IFCID: 007—SQL Errors</td>
</tr>
<tr>
<td>APSTACCS</td>
<td>Specify whether to collect APPTUNE statement accounting summaries data.</td>
<td>APPTUNE/SQL Performance Accounting Statement Summary records: (BMC IFCIDs 308-310)</td>
</tr>
<tr>
<td>APSTMT</td>
<td>Specify whether to collect APPTUNE statement text, host variables, and exceptions data.</td>
<td>APPTUNE/SQL Performance BMC IFCIDs: 004—SQL Exceptions 005—SQL Statement Text 010—Host Variables 011—Object Statistics per SQL Exception</td>
</tr>
<tr>
<td>DB2ACCT</td>
<td>Specify whether to collect DB2 accounting data.</td>
<td>DB2 accounting records. DB2 IFCIDS: 003—Accounting 239—Package Accounting DBRMs</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Related IFCIDs</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DB2AUDIT</td>
<td>Specify whether to collect DB2 audit data.</td>
<td>DB2 audit records. DB2 IFCIDs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>140—Audit Authorization Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>141—Audit GRANTs and REVOKEs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>142—Audited Object DDL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>143—Audited Object First Write Attempt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>144—Audited Object First Read Attempt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>145—Audited Object DML at BIND</td>
</tr>
<tr>
<td></td>
<td></td>
<td>146—User-Defined Audit Trace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>312—Audit Trail for DCE Security Processing</td>
</tr>
<tr>
<td>DB2PERF</td>
<td>Specify whether to collect DB2 performance data.</td>
<td>DB2 Performance Records (all other DB2 IFCIDs)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MainView for DB2 - Data Collector IFCIDs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>023-025—Utility Processing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>090—Text of DB2 Command</td>
</tr>
<tr>
<td></td>
<td></td>
<td>173—ASUTIME Exceeded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>125—RID List Processing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>225—Storage Summary</td>
</tr>
<tr>
<td>DB2SYS</td>
<td>Specify whether to collect DB2 statistics events data.</td>
<td>DB2 system records. DB2 IFCIDs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>001—System Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>002—Database Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>031—EDM Pool Full Condition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>054—Lock Contention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>102—Start Short on Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>103—End Short on Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>104—Log Data Set Names</td>
</tr>
<tr>
<td></td>
<td></td>
<td>105—DBID/OBID Translate to Names</td>
</tr>
<tr>
<td></td>
<td></td>
<td>106—System Parameters (DSNZPARM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>107—Page Set OPEN/CLOSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>172—Deadlock Detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>196—Timeout Detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>199—Data Set I/O Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>202—Statistics Dynamic DSNZPARMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>203—Heuristic Decision (DDF COMMIT/ABORT)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>204—Partner COLD START Detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>206—SNA Compare States (CS) Protocol Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>205—WARM START logname or syncpoint error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>206—SNA Compare States (CS) Protocol Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>207—Heuristic Damage During CS Exchange</td>
</tr>
<tr>
<td></td>
<td></td>
<td>208—SNA Syncpoint Protocol Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>209—Syncpoint Communication Failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>210—LOGNAME Changed on WARM START</td>
</tr>
<tr>
<td></td>
<td></td>
<td>230—Global Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>232—Thread Entry or Exit from DB2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>233—Start/End Call Stored Procedure Server</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Related IFCIDs</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DCSYSTEM</td>
<td>Specify whether to collect DATA Collector events data.</td>
<td>Data Collector events. BMC IFCIDs: 241—Command Response 245—DB2 WTO Messages</td>
</tr>
<tr>
<td>MVDBACC</td>
<td>Specify whether to collect MainView for DB2 - DC accounting summary data.</td>
<td>MainView for DB2 - Data Collector Accounting Summary Records (BMC IFCIDs 350-352)</td>
</tr>
<tr>
<td>OPERTUNE</td>
<td>Specify whether to collect OPERTUNE events data.</td>
<td>OPERTUNE records (BMC IFCID 17)</td>
</tr>
</tbody>
</table>

a This IFCID is disabled by default. It can be used optionally for batch reporting. See the MainView for DB2 Performance Reporter User Guide for instructions on how to activate additional IFCIDs when you want to produce a report that requires them.

b If you are installing Pool Advisor or the Pool Advisor component of System Performance for the first time, ensure that the PAHIST data class is included in an output group for each DB2 that will be involved in Pool Advisor reporting.

Specify the NGL LOGSET parameters associated with the output group.

a Expand the NGL LOGSET Parameters section.

b Specify the values described in Table 108 on page 259. These values define the LOGSETs that the NGL will use when collecting and archiving data.
Table 108: NGL LOGSET parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGSET compression</td>
<td>Specify whether log file data will be compressed, and if so, to what degree.</td>
</tr>
<tr>
<td>▪ Low (default)</td>
<td>A selection of <strong>LOW</strong> (default), is considered the optimal balance of compression and CPU usage.</td>
</tr>
<tr>
<td>▪ High</td>
<td>A selection of <strong>HIGH</strong> will save more DASD space but use significantly more CPU (including zIIP usage where available).</td>
</tr>
<tr>
<td>▪ No</td>
<td>A selection of <strong>NO</strong> disables compression, saving CPU usage at the expense of DASD space.</td>
</tr>
<tr>
<td>LOGSET time span</td>
<td>Specify the LOGSET time span in days (D), hours (H), or minutes (M). You can only specify one type of time D, H, or M. If you specify a number</td>
</tr>
<tr>
<td></td>
<td>without a type, the value defaults to days.</td>
</tr>
<tr>
<td></td>
<td>This value specifies the amount of time that you would like to have data kept in log files. If the log files are all filled up in less time</td>
</tr>
<tr>
<td></td>
<td>than this target value, more log files will be allocated up to the Max LOGSET data sets specified.</td>
</tr>
<tr>
<td>Max log buffers</td>
<td>Specify the maximum number of log I/O buffers that are used. Valid values are from 2 through 20.</td>
</tr>
<tr>
<td>Max read buffers</td>
<td>Specify the maximum number of read I/O buffers that are used. Valid values are from 2 through 99.</td>
</tr>
<tr>
<td>Deferred write time</td>
<td>Specify the deferred write time. The deferred write time is the maximum time delay before buffered records are written to the DASD log files.</td>
</tr>
<tr>
<td></td>
<td>Shorter deferred times mean less vulnerability to data loss in the event of an outage, but it requires more write I/Os. Valid values are from 1</td>
</tr>
<tr>
<td></td>
<td>through 999 seconds.</td>
</tr>
<tr>
<td>Minimum log file data sets (LDS)</td>
<td>Specify the minimum number of data sets to use in the LOGSET. The NGL agent will allocate this number of data sets at start up. Valid values</td>
</tr>
<tr>
<td></td>
<td>are from 1 through 99.</td>
</tr>
<tr>
<td>Maximum log file data sets (LDS)</td>
<td>Specify the maximum number of data sets to use in the LOGSET. The NGL agent will allocate up to this number of data sets, as needed, to meet</td>
</tr>
<tr>
<td></td>
<td>the retention goal specified in the LOGSET time specification. Valid values are from 1 through 99.</td>
</tr>
<tr>
<td>Space to allocate (per LDS)</td>
<td>Specify the total space used for the LOGFILE. This space is used to create each LOGFILE data set. Valid values are from 1 through 9999 MB.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LDS allocation type</td>
<td>Specify the type of allocation parameters to be used.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>SMS</strong> means that DFSMS parameters will be used and at least one of the 3 SMS parameters (storage class, management class, data class) must be provided.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>VOL</strong> means that a traditional VOLSER will be provided to indicate where the LOGFILE should be allocated.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>NONE</strong> means that no allocation parameters will be provided and the system defaults will handle the details.</td>
</tr>
<tr>
<td>LDS Volume</td>
<td>Specify the volume for the LOGSET. This value is required if the allocation type is <strong>VOL</strong>; otherwise, this value is ignored.</td>
</tr>
<tr>
<td>LDS DFSMS Data class <em>(optional)</em></td>
<td>Specify the DFSMS Data class for the LOGSET.</td>
</tr>
<tr>
<td></td>
<td>You must specify one of the LDS DFSMS parameters if the allocation type is <strong>SMS</strong>. This parameter is ignored if the allocation type is not <strong>SMS</strong>.</td>
</tr>
<tr>
<td>LDS DFSMS Management class <em>(optional)</em></td>
<td>Specify the DFSMS Management class for the LOGSET.</td>
</tr>
<tr>
<td></td>
<td>You must specify one of the LDS DFSMS parameters if the allocation type is <strong>SMS</strong>. This parameter is ignored if the allocation type is not <strong>SMS</strong>.</td>
</tr>
<tr>
<td>LDS DFSMS Storage class <em>(optional)</em></td>
<td>Specify the DFSMS Storage class for the LOGSET.</td>
</tr>
<tr>
<td></td>
<td>You must specify one of the LDS DFSMS parameters if the allocation type is <strong>SMS</strong>. This parameter is ignored if the allocation type is not <strong>SMS</strong>.</td>
</tr>
<tr>
<td>LDS DSN prefix</td>
<td>Specify the DSN prefix for the LOGSET log file data sets.</td>
</tr>
<tr>
<td></td>
<td>BMC recommends referencing the <strong>Data Collector ID</strong> and <strong>Output Group Number</strong> in the DSN prefix to make it unique (for example, BMCPERF.DC01.OG001).</td>
</tr>
<tr>
<td>Enable Archiving</td>
<td>Specify whether to enable LOGSET data set archiving. Valid values are <strong>Y</strong> (Yes) and <strong>N</strong> (No).</td>
</tr>
<tr>
<td></td>
<td>For more information about archiving, see “Additional information about archiving and the NGL” on page 269.</td>
</tr>
<tr>
<td>Archive Wait Time <em>(optional)</em></td>
<td>Specify the maximum time in seconds to wait for an archive to finish before reusing a LOGFILE. Allowed values are 1-9999 with the default value of 600 seconds.</td>
</tr>
<tr>
<td>Archive post processing job <em>(optional)</em></td>
<td>Specify the member that contains the job that executes when the archive job is done. The data set that contains the member is defined by the DOMPARMS DD in the DBC started task.</td>
</tr>
<tr>
<td></td>
<td>For more information about the post-processing job, see “Additional information about archiving and the NGL” on page 269.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max days to keep archives</td>
<td>Specify the number of days that archive data sets are kept. You can specify 1 to 999 days, or specify 0 (zero) for no limit.</td>
</tr>
<tr>
<td>Max numbers of archives to keep</td>
<td>Specify the number of archived data sets that are kept. You can specify 1 to 999, or specify 0 (zero) for no limit.</td>
</tr>
<tr>
<td>Max combined size of archives</td>
<td>Specify the maximum DASD space usage allowed in all archives. You can specify 1 to 999999 MB, or specify 0 (zero) for no limit.</td>
</tr>
<tr>
<td>Archive file Allocation type</td>
<td>Specify the type of allocation parameters to be used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SMS</strong> means that DFSMS parameters will be used. At least one of the three SMS parameters (storage class, management class, data class) must be provided. If you select this value, VOL and UNIT parameters are ignored.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VOL</strong> means that a traditional VOLSER will be provided to indicate where the LOGFILE should be allocated, and SMS parameters are ignored.</td>
</tr>
<tr>
<td></td>
<td>• <strong>UNIT</strong> means that a traditional UNIT will be provided to indicate where the LOGFILE should be allocated, and SMS parameters are ignored.</td>
</tr>
<tr>
<td>Archive Volume (optional)</td>
<td>Specify the volume for the archive.</td>
</tr>
<tr>
<td>Archive DFSMS Data class (optional)</td>
<td>Specify the DFSMS data class.</td>
</tr>
<tr>
<td>Archive DFSMS Management class (optional)</td>
<td>Specify the DFSMS management class for the archive.</td>
</tr>
<tr>
<td>Archive DFSMS Storage class (optional)</td>
<td>Specify the DFSMS storage class for the archive.</td>
</tr>
<tr>
<td>Archive GDG</td>
<td>Specify the GDG element to control whether ARCPREFIX or ARCDSN is the base name for a generation data group. Valid values are <strong>Y</strong> (Yes) and <strong>N</strong> (No). You must specify GDG as <strong>Y</strong> if the archive output data set is to be a member of a generation data group. The archive program will create a +1 version for the output data set.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Archive DSN prefix *(optional)* | Specify the DSN prefix for the NGL archive data set.  
*Note:* Instead of this field you can specify a fully qualified DSN for the archive by specifying an archive data set prefix in the Alternate full archive DSN option. The Archive DSN prefix and Alternate full archive DSN options are mutually exclusive.  
BMC recommends referencing the Data Collector ID and Output Group Number in the DSN prefix to make it unique (for example, BMCPERF.DC01.OG001). A sequence number prefixed by the letter A will be appended as the last node. |

| Alternate full archive DSN *(optional)* | Specify the fully qualified NGL archive data set name.  
*Note:* Instead of this field you can specify an archive data set prefix for the archive by using the Archive DSN prefix option. The Archive DSN prefix and Alternate full Archive DSN options are mutually exclusive.  
BMC recommends referencing the Data Collector ID and Output Group Number as well as using date and time symbolics to make the data set name unique each time (for example, BMCPERF.DC01.OG001.D&JDAY..T&HHMMSS). |

Specify the DB2 SSIDs associated with this group:

a Place your cursor on the > (greater than) sign next to Subsystems supported by this group and press Enter.

b At the Zoom panel, specify up to 63 DB2 SSIDs for the DB2 subsystems supported by this output group.

You can also specify * to associate all DB2 subsystems in your DB2 Monitor List with this output group. Any DB2 subsystems that are running on a different system are ignored.

c Press F3 to return to the previous panel when finished.

**Verifying or changing DOMPLEX parameters**

This task is **required** for a new product installation. It is **optional** for a migration installation.

The DOMPLEX parameters affect all users and procedures that use the same DOMPLEX option set.
To verify or change DOMPLEX parameters

1. At your product main menu, select Administration.

2. At the Administration menu, select 2 (DOMPLEX Option Sets) and press Enter.

3. At the DOMPLEX Options Sets panel, type E next to the DOMPLEX for which you want to define values and press Enter.

4. At the DOMPLEX options set panel, expand DOMPLEX Parameters, as shown in Figure 37 on page 263.

Figure 37: DOMPLEX option set panel — Expanded DOMPLEX parameters

5. Specify the parameters, as described in Table 109 on page 263.

Table 109: DOMPLEX Parameters fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sysplex communications enabled</td>
<td>Specify whether the Data Collector on the current system will connect to an XCF group in the coupling facility, and subsequently establish communication with all Data Collectors in the DOMPLEX. Valid values are Y (Yes) and N (No). The default is Y.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Global data transfer limit</td>
<td>Specify the maximum size (in megabytes) of a request that can be transferred to a remote system. Any request that exceeds the specified limit specified will be terminated. Valid values are any number in the range 1 through 999. The default value is 20. For information about data transfer limits, see “Data transfer limit calculations” on page 265.</td>
</tr>
<tr>
<td>Local data transfer limit</td>
<td>Specify the maximum size (in megabytes) of a request that can be transferred to a user on the local system. Any request that exceeds the limit will be terminated. Valid values are any number in the range 1 through 999. The default value is 50. For information about data transfer limits, see “Data transfer limit calculations” on page 265.</td>
</tr>
<tr>
<td>(MainView for DB2 only)</td>
<td>Collect IFCID 3 in accounting trace Specify whether to collect IFCID 3 in accounting trace. Valid values are Y (Yes) and N (No).</td>
</tr>
<tr>
<td>Security via DB2 authorization tables</td>
<td>Specify whether security through the DB2 authorization tables is enabled. Valid values are Y (Yes) and N (No).</td>
</tr>
<tr>
<td>Authorization for DB2 commands</td>
<td>Specify whether authorization is required for DB2 commands. Valid values are Y (Yes) and N (No).</td>
</tr>
<tr>
<td>Authorization for MVS commands</td>
<td>Specify whether authorization is required for MVS commands. Valid values are Y (Yes) and N (No).</td>
</tr>
<tr>
<td>Translate all panels to upper case</td>
<td>Specify whether System and SQL Performance product panels are displayed in both upper- and lower-case characters or only in upper-case characters. This value sets the default for users who do not set a preference in their profile.  ■ Specify Y to display panels and reports in upper-case characters.  ■ (default) Specify N to display panels and reports in mixed case. Note: This setting does not apply to SQL Explorer-specific reports and panels or Explain reports. It does apply to panels shared by SQL Explorer with other System and SQL Performance products.</td>
</tr>
<tr>
<td>Site Panel Language identifier</td>
<td>Specify the language used on System and SQL Performance product panels. This field acts as the default for all users who do not set a preference in User Options or the User Profile. Specify E (English) or J (Japanese).</td>
</tr>
</tbody>
</table>
6 Press F3 until you return to the Administration menu.

7 If prompted, enter the name of the DOMPLEX and a description.

### Data transfer limit calculations

The local transfer limit controls how much local storage a user data request can occupy from a single request for data. This limit ensures that a single user cannot use too much of the Data Collector private storage area for a single request.

The global transfer limit controls how much data a Data Collector will attempt to return to a remote Data Collector for a single data request from a remote user. This transfer limit controls the demand on Coupling Facility resources. Because the entire
request for data from all DB2 subsystems must be satisfied from within the local transfer limit buffer, the local transfer limit must always be larger than the global limit.

Because concurrent users may be issuing simultaneous requests, each request can potentially use up to that amount of storage. If the local transfer limit is set too high, and your environment has many concurrent users, simultaneous requests can exceed the private virtual storage capacity of the Data Collector and cause it to fail.

Typical z/OS systems provide between 1300 MB and 1600 MB of available private storage, so a value of 1000 MB is a good working maximum for all concurrent user requests combined. Because this storage must be balanced between the number of active user requests and the size of those requests, 1000 MB can support a limit of 50 MB for 20 simultaneous requests. If the limit is increased to accommodate a large user request, you must then decrease the number of users. For example, increasing the limit to 100 MB results in only 10 simultaneous user requests that obtain the maximum amount of data.

If you have a large number of concurrent users, the size of the user requests should be reduced. You can reduce the actual size of the request, or consider requesting the data from a batch report request. Batch report requests that do not use the Data Collector as their source are not subject to these limitations.

If you are changing the default limits, use the following considerations in your calculations:

- The combination of local transfer limits for all users and the global transfer limits for all DB2s should never exceed 1000 MB.
- The higher the local transfer limits, the lower the number of users that will be using those limits.
- The global transfer limit should always be lower than the local transfer limit.

**Checking the default User Profile**

User Profiles define the operating characteristics for a product session, including the authorizations granted to individual users.

To make the job of administration easier, the product automatically generates a User Profile the first time a user tries to sign on by copying the default User Profile loaded during installation (called 9DEFAULT).
WARNING

The 9DEFAULT records shipped in the SECURITY and PROFILE data sets contain default values that grant maximum authority to users. If you want to use the 9DEFAULT profile but do not want all users to have maximum authority, you must modify the 9DEFAULT profile before users access the product. Alternatively, you can delete the 9DEFAULT profile to prevent unauthorized access. BMC recommends that you copy the 9DEFAULT profile to another profile (8DEFAULT, for example) and create a User Profile with maximum authority for yourself first.

Before making the product available to multiple users in your environment, check the authorizations in the 9DEFAULT profile to make sure they are consistent with the security strategy at your site. User Profiles are discussed in detail in the System and SQL Performance for DB2 Administrator Guide.

Extensive online Help exists for all panels and their associated fields. If you press F1 while the cursor is positioned on a text-only area of a panel, a description of that panel is displayed. If you press F1 while the cursor is positioned on an input or output field on a panel, specific information about that field is displayed.

To view and modify User Profile values

1. Select option 1 (User Profiles) from the Administration menu.

   The User Profile Administration panel (Figure 38 on page 267) is displayed.

   **Figure 38: User Profile Administration panel**

<table>
<thead>
<tr>
<th>DOMEPRFU/P</th>
<th>User Profile Administration</th>
<th>LINE 195 OF 196</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ====&gt; _______________________________________________ Scroll ===&gt; CSR_</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   To add a profile, type the name in the "New profile" field, and/or type one or more action codes. Then press Enter.

   V - View  M - Modify  D - Delete  C - Copy

   New profile

<table>
<thead>
<tr>
<th>Act</th>
<th>Name</th>
<th>Description</th>
<th>Last change date</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>USER01</td>
<td>DEFAULT PROFILE</td>
<td>1998-10-14 07:58</td>
<td>9DEFAULT</td>
</tr>
<tr>
<td>_</td>
<td>9DEFAULT</td>
<td>DEFAULT PROFILE</td>
<td>1998-10-08 11:03</td>
<td>BMCSftwr</td>
</tr>
</tbody>
</table>

2. Move the cursor to the Act field beside the User Profile of the product administrator. Type M (Modify) and press Enter.

   The User Profile Data Menu (Figure 39 on page 267) is displayed.

   **Figure 39: User Profile Data Menu**

<table>
<thead>
<tr>
<th>DOMEUPRO/I</th>
<th>User Profile Data Menu</th>
<th>15:46:29</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command ====&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   User name : USER01

   Type an optional description for this user in the field below.

   Description  DEFAULT_PROFILE  ______________
Select one of the following options. Then press Enter.

- A. Authorization - Display authorization values that can be set only by an administrator.
  1. Session Control - Parameters that control the user's session
  2. Not available

The following values cannot be locked from user update.

- 3. Session Options - Parameters that customize the session
- 4. Presentation Options - Parameters that control language and formatting
- 5. Function Keys - Function key values

3 Press F3 to exit.

A confirmation panel is displayed.

4 Select option 1 (Save changes) and press Enter.

**Note**

An individual security record is not created until a User Profile is modified. By opening and saving the User Profile of the product administrator before modifying the 9DEFAULT User Profile, you ensure that the administrator retains maximum authority.

5 Repeat Step 2 on page 267 through Step 4 on page 268, selecting the 9DEFAULT User Profile.

6 Review each option on the User Profile Data Menu carefully, especially option A (Authorization) and option 1 (Session Control).

- Use **Authorization** (option A) to display authorization values that can be set only by an administrator:
  - Data Collector access
  - DB2 access
  - Product access

- Use **Session Control** (option 1) to set the parameters that control access to product functions and limit resource use.

- Use **Session Options** (option 3) to set characteristics for the user's session (for example, placement of **Command** line and display of panel ID).

- Use **Presentation Options** (option 4) to set the parameters that control the presentation of data on your screen (for example, upper- or mixed-case, date style, and decimal style).

- Use **Function Keys** (option 5) to set function key defaults.

7 Press F3 to exit the User Profile Data Menu.
A confirmation panel is displayed.

8 Select option 1 to save your changes.

9 Press F3 until the main menu is displayed. Leave your product session active.

**Additional information about archiving and the NGL**

You can setup a procedure to automatically generate an archive of a log file, and setup a post processing job that is automatically submitted each time an archive procedure finishes.

The archives are automatically registered in the Archive Directory and can be used to create the batch reports described in the following books:

- *APPTUNE for DB2 User Guide*
- *Pool Advisor for DB2 User Guide*
- *BMC System Performance for DB2 User Guide*
- *MainView for DB2 Performance Reporter User Guide*

When enabled, the Data Collector initiates a procedure to create an archive of a log file, when any of the following conditions occur:

- A log file is full
- The SWITCH command is issued

To enable archiving:

1 Set **Enable Archiving** to **Y** on the output group that you are interested in archiving.

2 Copy the NGLARCH member from *HLQ.LLQSAMP* into your SYS1.PROCLIB (or equivalent) started task library.

**Note**

The default name for this process is NGLARCH. You can change the process name. For more details, see “Renaming the NGLARCH process” on page 270.

In addition, you can configure an archive post-processing job that is automatically submitted each time an archive procedure finishes. For more details, see “Setting up an archive post-processing job” on page 270.
Renaming the NGLARCH process

You can change the name of the NGLARCH process.

1. Edit installation job $465INIT.

2. Change the <PROCNAME> value to the new name of the NGLARCH proc.

3. Rerun the NGLINIT step while the DBC is up.

Setting up an archive post-processing job

You can configure an archive post-processing job (#DOMPOST) that is automatically submitted each time an archive procedure finishes.

1. Set up the job as a member of the dataset specified on the DOMPARMS DD of the DBC started task.

2. Specify the member name in the Archive post processing job field in the DOMPLEX option set.

The symbols in Table 110 on page 270 are supported in the optional archive post-processing job. The product replaces these symbols in the JCL with the appropriate values when the job is submitted for execution.

--- Note ---

All the $DOM symbols are optional in the post-processing jobs.

Table 110: Symbols used in archive post-processing jobs

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Substituted value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$DOMSSN</td>
<td>Current DBC subsystem ID</td>
</tr>
<tr>
<td>$DOMDSN</td>
<td>Current trace data set name</td>
</tr>
<tr>
<td>$DOMDATE</td>
<td>Current date in the format Dyyddd, where yy is the year (00–99) and ddd is the day of the year (000–365)</td>
</tr>
<tr>
<td>$DOMTIME</td>
<td>Current time in the format TMhhmmss, where hh is hours (00–23), mm is minutes (00–59), and ss is seconds (00–59)</td>
</tr>
<tr>
<td>$DOMLSET</td>
<td>LOGSET name</td>
</tr>
<tr>
<td>$DOMPLX</td>
<td>Current DOMPLEX name (specified in the DOMPLEX option set)</td>
</tr>
<tr>
<td>$DOMARC</td>
<td>Archive data set name or $NULLFILE if no archive is generated</td>
</tr>
<tr>
<td>$DOMARCN</td>
<td>Archive data set name that was generated even if no archive is produced</td>
</tr>
</tbody>
</table>
You can substitute substrings of these symbols, using the substring function:

$\text{SUBSTR}(ss, ll, vvvvvv)$

The syntax of the substring function is:

- The $ss$ value represents the starting position.
- The $ll$ value represents the length.
- The $vvvvvv$ value is a symbol name.

For example, to represent the first 10 characters of $\text{DOMDSN}$:

$\text{SUBSTR}(1, 10, \text{DOMDSN})$

---

**Note**

You can find asample post-processing job (#DOMPOST) in the DOMSAMP, BBSAMP, or runtime SAMP data set, along with a REXX EXEC (DOMRPOST) that you can use to display these symbolics.

---

**Customizing the OPERTUNE for DB2 product**

This section outlines the post-installation and customization tasks that are necessary for the successful completion of OPERTUNE for DB2 installation.

**Copying the OPERTUNE procedure to a PROCLIB**

This *required* task copies the OPERTUNE started task procedure needed to a PROCLIB. Each maintenance level of OPERTUNE requires only one started task procedure per z/OS. The Installation System customizes the member DDTPROC in the output JCL data set.

**To copy the OPERTUNE procedure to a PROCLIB**

1. Copy the DDTPROC member to a PROCLIB at your installation.

2. Ensure that the DDTPROC member contains the appropriate DD statements.

   The procedure uses the following DD statements:

   - *(required)* DDTPROFS references the OPERTUNE profile data set that contains user, system, and security profiles.
■ **(required)** DDTAUDIT logs the changes made to all subsystems by this OPERTUNE and provides an audit trace.

By default, the log is written to SYSOUT. To write the audit log to DASD, preallocate a data set with the following attributes:

- LRECL=121
- RECFM=FB
- DSORG=PS

If you allocate the data set in the OPERTUNE procedure with DISP=MOD, you must periodically check and empty the data set to prevent it from filling up. If you specify DISP=OLD, you must copy the data set each time OPERTUNE is terminated.

If you write the audit log to a data set, specify DCB=BUFNO=1 on the DD statement to prevent buffering from occurring. You must make this specification to be able to view the latest OPERTUNE logged changes through the ISPF Browse option. In addition, if you perform an IPL on the z/OS system while OPERTUNE is still running, some OPERTUNE changes might not be logged to the data set.

■ **(optional)** DDTTRACE provides internal trace information for diagnostic purposes. Like DDTLOG, these traces could be output to SYSOUT or to DASD. The default is SYSOUT and is recommended. If you want to write the traces to DASD, preallocate a data set with the following attributes:

- LRECL=121
- RECFM=FB
- DSORG=PS

■ **(optional)** DDTTRACS provides a log to track the security profile created by the OPERTUNE security exit. Like DDTAUDIT, these traces could be output to SYSOUT or to DASD. The default is SYSOUT and is recommended. If you want to write the traces to DASD, preallocate a data set with the following attributes:

- LRECL=121
- RECFM=FB
- DSORG=PS

3 If you are installing a maintenance upgrade, cycle the OPERTUNE started task and any ISPF sessions, using OPERTUNE to activate the new code.
For the purpose of canceling threads, BMC Software recommends that you run OPERTUNE at a dispatching priority higher than any DB2-allied address spaces. Code the appropriate DPRTY parameter [for example, DPRTY=(n,m)] on the EXEC statement of the OPERTUNE procedure.

**Invoking the OPERTUNE CLIST or the common BMCDISPN panel**

This *required* task enables the OPERTUNE CLIST or common BMCDISPN panel. Each maintenance level of OPERTUNE requires only one CLIST per z/OS.

**Note**
The BMCDISPN panel is located in the output JCL data set.

### To invoke the OPERTUNE CLIST or the common BMCDISPN panel

1. If the ISPF module ISPLINK does not reside in an ISPLLIB library, a STEPLIB library, the LPALIB, or the LINKLIST and you do not want to copy ISPLINK to one of these libraries, modify the OPERTUNE CLIST DDTCLIST to concatenate DDTLOAD with the library where ISPLINK is located as follows:
   ```
   ALLOC F(DDTLOAD) DA('HLQ1.LOAD' 'SYS1.ISPLOAD') SHR REUSE
   ```
   
   *HLQ1* is the high-level qualifier of your OPERTUNE load library.

   The Installation System customizes the member DDTCLIST in the output JCL data set.

2. Copy the member to a CLIST library at your installation.

   If your installation uses variable-block (VB) CLISTs rather than fixed-block (FB) CLISTs, you can re-block the CLIST by executing DDTRBLK, which is provided in the *LLQSAMP* (where *LLQ* is DB, XX, BB, and UBB) data set. Execution of DDTRBLK allocates a new VB CLIST, so you need to modify DDTRBLK to provide old and new high-level qualifiers for data sets and a volume for the allocation of the new CLIST library.

3. Invoke the OPERTUNE CLIST from TSO in one of the following ways:
   - Use `%DDTCLIST`.
   - Make OPERTUNE available from an ISPF menu by modifying ISR@PRIM or an equivalent panel, as follows:
1 In the )BODY area, add the following line:

```
%0   + BMC OPERTUNE
```

2 In the )PROC area, add the following line:

```
O,'CMD/DDTCLIST)' /* OPERTUNE USING LIBDEF */
```

The LIBDEF option is required to support multiple OPERTUNE systems at different maintenance levels.

- Use the panel customized by the Installation System that provides access to any or all of the System and SQL Performance products. If you use it, modify ISR@PRIM or an equivalent panel as follows:

1 In the panel area, add the following line:

```
%P + SYSTEM AND SQL PERFORMANCE PRODUCTS FOR DB2
```

2 In the )PROC area, add the following line:

```
P,'PANEL(BMCDISPN)'
```

4 Exit and reenter ISPF.

5 Select option P from the install system main menu or an equivalent panel to invoke the System and SQL Performance products.

## Creating an OPERTUNE system profile

Before you can access an OPERTUNE system, you must create a system profile.

An OPERTUNE system runs as a started task, not as a z/OS subsystem. See the OPERTUNE for DB2 Reference Manual for a discussion about creating system profiles.

This task is required for full installation.

### To create a system profile

1 From the OPERTUNE Miscellaneous Selection Menu, select option 2 (OPERTUNE System Profiles).

2 Type `ADD` and the new system name on the `Command` line of the Profile Selection List panel. Use the four-character OPERTUNE identifier specified during execution of the installation dialog.

3 Create additional system profiles as needed.
Defining security for OPERTUNE

This task defines security for using OPERTUNE. The task is required for full installation and optional for maintenance installation.

OPERTUNE secures its features through OPERTUNE user and security profiles. It also provides a security exit to interface with other security packages, such as RACF and CA-ACF2. The SAF interface is required in order to use the default security exit.

You can use OPERTUNE security, the security interface exit, or a combination of both. When you install OPERTUNE, the DEFAULT security profile is created. Two user profiles called * and DDTOPER are also created. See the OPERTUNE for DB2 Reference Manual for information about using the security interface exit and setting up security profiles.

To define security

1 Select option 8 (Administrative Utilities) from the OPERTUNE Main Selection Menu by typing 8 on the Command line and pressing Enter.

2 Select option 12 and indicate N/A as the primary target OPERTUNE.

3 When the Miscellaneous Selection Menu is displayed again, select option 3 (Security Profiles).

4 Create a security profile with full authority for the installer:
   a Type ADD profileName (where profileName is a name of your choice) on the Command line of the Profile Selection List panel, and press Enter. (For more information about creating a security profile, see the OPERTUNE for DB2 Reference Manual.)
   b Copy the DEFAULT security profile into this new security profile by typing COPY DEFAULT on the Command line.
   c Save your new security profile.

5 Create a user profile with full authority for the installer by typing ADD userProfile (where userProfile is a name of your choice) on the Command line of the Profile Selection List panel. Specify the security profile that you created in Step 4 on page 275. See the OPERTUNE for DB2 Reference Manual for details about creating a user profile.

The * user profile that OPERTUNE creates during installation does not specify a security profile, so the DEFAULT security profile is used. The DEFAULT security profile provides full update authority to all subsystems of the user.
The * user profile is used by any new user invoking the OPERTUNE dialog, if a specific user profile for that user ID has not been created. When that new user issues the first request to the target OPERTUNE, a new user profile for the new user’s ID is created, modeled after the * user profile. If only administrative functions are performed, no new profile is built and the DEFAULT profile continues to be used.

For these reasons, the values in the * user profile should be global. Review the * user profile and modify it to suit your environment. Delete the * user profile to restrict the authority of new users.

6 Review the DEFAULT security profile and modify it to suit your environment.

The DEFAULT security profile is created during initialization of the VSAM profile data set and has full authority. The DEFAULT security profile is used by any user invoking the OPERTUNE dialog unless a security profile has been specified in the user profile of that user. For this reason, the values in the DEFAULT security profile should be global.

7 Define a default operator profile named DDT OPER in the following situations:

- You decide to delete the * user profile to deny new users access through ISPF, but you want to allow operators to issue OPERTUNE commands from the operator console.
- You want your operators to have different authorizations than those of the * user profile.

8 After defining DDTOPER, define a security profile with the appropriate authority and specify the security profile in the DDTOPER profile. If neither the * user profile nor DDTOPER profiles are defined, only the MAINT command can be issued from the operator console. See the OPERTUNE for DB2 Reference Manual for more information on the MAINT command.

9 Create additional user profiles as needed.

Starting the OPERTUNE started task

This required task starts the OPERTUNE started task. A sample started task is in the output JCL data set member DDTPROC.

To start the OPERTUNE started task

1 From a system console, type one of the following commands:
S DDTPROC

If you are using a customized procedure, substitute the name of that procedure for DDTPROC.

S DDTPROC,SYS= opertuneID

The variable opertuneID is the four-character ID of an OPERTUNE system at your installation that is different from the default specified in the OPERTUNE procedure.

The following example shows the messages that appear during a normal startup of an OPERTUNE started task, where opID is the four-character OPERTUNE system ID, asID is the address space ID, and DB2ssid is the DB2 subsystem ID. These messages are issued in route code 11.

BMC31002I opID OPERTUNE Vv.r.mm, ASID(asID)- nnnnnnnn
BMC31154W opID OPERTUNE FOR type TRIAL WILL EXPIRE IN nn DAYS
BMC31300I opID NO VTAM APPLID SPECIFIED - VTAM OPERATIONS NOT POSSIBLE
BMC31500I opIDDB2ssid ACCEPTING WORK REQUESTS FOR DB2ssid
BMC31019I opID INITIALIZATION COMPLETE

Note
The messages might not appear in the order shown and might be accompanied by other messages.

When you are ready to terminate the OPERTUNE started task, type the following command, where opertuneID is the four-character OPERTUNE system ID:

P opertuneID

2 If you are installing a maintenance upgrade, cycle the OPERTUNE started task and any ISPF sessions, using OPERTUNE to activate the new code.

Note
OPERTUNE can also be run as a batch job.

Preparing ISPF for OPERTUNE diagnostics

This task enables OPERTUNE to obtain a dump for diagnostic purposes. OPERTUNE provides diagnostic panels in case an abend occurs in the ISPF dialog. However, you might need to obtain a dump to diagnose the problem.

To prepare ISPF for OPERTUNE diagnostics

Complete this task for each user of OPERTUNE.
1 From the ISPF Primary Option Menu, select option 0.

2 Select Environ from the action bar and modify the settings to enable a dump.

3 Ensure that your logon procedure has a SYSUDUMP DD statement specified, or use the TSO ALLOC command when the abend occurs to allocate a dump data set.

The following examples illustrate how to properly obtain a dump.

**Example 1**
The following command sends output to SYSOUT X:

```
TSO ALLOC FI(SYSUDUMP) CLASS(X)
```

**Example 2**
The following command sends output to a preallocated data set, where `HLQ` is a high-level qualifier of your choice:

```
TSO ALLOC FI(SYSUDUMP) DSN('HLQ.SYSUDUMP') OLD
```

---

**Establishing OPERTUNE communications**

Optionally, you can establish communications between two or more OPERTUNE systems.

**To establish OPERTUNE communications**

1 For detailed instructions, see the *OPERTUNE for DB2 Reference Manual*.
Customizing EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE

This chapter describes additional customization tasks that are specific for the EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE products.

Customizing XBM subsystems

This section describes how to customize the XBM subsystems and PROCs for XBM.

Completing XBM installation

To complete your installation of XBM, perform the following steps:

1. Copy the XBM PROC to a PROCLIB.

Each maintenance level of XBM requires one started-task procedure per XBM subsystem. The PROC is generated by the Installation System into a member in the JCL data set.

See “Defining and starting the XBM started task” on page 280 for detailed information about setting up the PROC.

**Note**

If you do not specify the value of the XBM SSID using the SYS parameter in the PROC, the XBM SSID will be the first four characters of the member name. For example, if the member name is XBMO15, the XBM SSID would be XBMO. For example, if you name your XBM subsystems XBMA, XBMB, and XPMC, you can specify the pattern XBM* as the XBM SSID value in the XBM$OPTS member to access all of these subsystems.
2 If you have a previous version of XBM active, cycle the XBM started task and any ISPF sessions to activate the new code.

3 Copy the XBM EXEC to a CLIST library.

The Installation System customizes the member XBMISPF in the JCL library. Options for XBMISPF are defined in XBM$OPTS, which is also located in the JCL library. XBM$OPTS is the default options member for XBMISPF. If you do not specify an options member when you run XBMISPF, the EXEC uses the XBM$OPTS member.

**Note**
You should place XBMISPF and XBM$OPTS in a system library (SYSPROC or SYSEXEC) accessible to TSO users.

4 If you want to create the common BMCDISP panel, modify ISR@PRIM or an equivalent panel, as follows:

In the )BODY area of your user CLIST, add the following entry:

```clist
%O + BMC XBM
```

In the )PROC area of the XBM SYSPROC library, add the following entry:

```clist
O,'CMD(XBMISPF)'
```

5 If you are using multiple XBM subsystems, create a separate XBM$OPTx member for each XBM subsystem. In each XBM$OPTx member, specify the name of the associated XBM subsystem in the XBMSSID parameter.

You could use pattern-matching characters in the XBMSSID parameter of the XBM$OPTS member and use a single XBM$OPTS member for all subsystems. To use pattern-matching characters, you must use a standard naming convention for your XBM subsystems so that the pattern can match multiple subsystem names.

For more information, see “Customizing XBM$OPTS for data sharing environments” on page 287.

### Defining and starting the XBM started task

XBM started tasks are initialized by submitting the started-task procedure. More than one XBM subsystem can be started by using single or multiple procedure members.
To create an XBM procedure in your system library

1. Copy the XBM PROC from the install HLQ/JCL to your system PROCLIB (where HLQ is the high-level qualifier you specified during installation).

2. Edit the PROC parameters as desired. You do not need to change the parameters before you start XBM for the first time.

Figure 40 on page 281 shows an example of the JCL for the procedure.

**Figure 40: Sample of JCL for XBM started task**

```plaintext
//XBM         PROC CONFIG='*',MS=,XBMGRP=,SYS=,XSSI=
//*===================================================================
//*           (C)COPYRIGHT 1993 - 2013 BMC SOFTWARE
//*           AS AN UNPUBLISHED WORK.
//*===================================================================
//XBM         EXEC PGM=XBMXMAIN,REGION=0M,TIME=1440,
//            PARM=('CONFIG=&CONFIG MS=&MS ',
//            ' XBMGROUP=&XBMGRP SYS=&SYS SSI=&XSSI')
//********************************************************************
//STEPLIB     DD DISP=SHR,DSN=hlq.XBMLINK           (xbm/Solution loadlib)
//            DD DISP=SHR,DSN=hlq.BBLINK            (BMC Security modules)
//BMCPSWD     DD DISP=SHR,DSN=securityLibraryName     (if used for auth)
//SYSPRINT    DD SYSOUT=*,DCB=RECFM=VA
//XBMXINIT    DD DUMMY  *** XBM.INITIALIZATION.COMMAND.FILE  ***
//PROIGN      DD DUMMY
//X37IGN      DD DUMMY
//XBMXTASK    DD DISP=SHR,DSN=yourlib.SIBLINK
//            DD DISP=SHR,DSN=yourlib.SIBLOAD
//            DD DISP=SHR,DSN=yourlib.STKLOAD
//XBMREP01    DD DISP=SHR,DSN=hlq.VSAM.XBMREP01
//XBMREP02    DD DISP=SHR,DSN=hlq.VSAM.XBMREP02
```

**Note**

You must specify the location of the modules for security password checking and for authorization:

- You must include the location of the security modules in the XBM STEPLIB or the linklist. The security modules are typically located in the XBM.BBLINK library.

- You can specify the location of the authorization modules by either including them in an XBM STEPLIB library or in the LINKLIST, or by using the BMCPSWD DD statement and including them in the specified library.

3. Submit the JCL to start the XBM subsystem.

**Parameters**

This section describes the parameters that the XBM procedure accepts.
CONFIG

The first time that you start XBM, you do not have a configuration file to specify. Consequently, XBM activates the DEFAULT_CONFIG configuration. During subsequent restarts, if you do not specify a CONFIG parameter, XBM activates the last active configuration.

MS

The first time that you start XBM, you do not have a management set (MS) to specify. Because management sets do not have default values, a management set does not activate automatically. During subsequent restarts, XBM activates a management set only if you specify it or add the ACTIVATE commands to your XBMXINIT data set.

XBMGROUP

This parameter specifies the name of the cross-system coupling facility (XCF) group that you want this XBM subsystem to join when the PSS component is started, if applicable. This name must match the first level of the structure name for the XBM structures defined in your coupling facility resource manager (CFRM) policy. The first time that you start XBM, the default for this parameter is XBMGROUP.

If you specify an XCF group name by using this parameter, you must perform the following tasks before the XBM subsystem can join the group:

1. Set the Join sysplex group when PSS started option to Yes on the PSS Options subpanel.
2. Start the PSS component.

Note

The XBMGROUP parameter overrides any XCF group name that you enter in the Sysplex group name field on the PSS Options subpanel. If you enter an XCF group name on the MVS command to start the XBM started task, that group name overrides the XBMGROUP parameter and the group name on the PSS Options subpanel.

SYS

The XBM subsystem name (identified as XBMID by DB2 utilities, or XBMSSID by IMS utilities) is the first four characters of the started-task procedure, or it is the name specified with the SYS parameter (a maximum of four characters). The SYS parameter takes higher precedence.

This subsystem name must:

- Start with a letter
Be two to four characters in length
Contain only the letters A-Z, the numbers 0-9, $, or #

**Note**

Note the following considerations when setting up your system name:

- If you specify an invalid value in the SYS parameter, XBM starts the subsystem by using the first four characters of the name of the started task or job as the XBM subsystem name. For example, if your site has naming conventions that require you to name the started task `DB2AXBM` (where `DB2A` is a valid DB2 subsystem name), the SYS parameter lets you name your XBM subsystem so that it does not conflict with the DB2 subsystem name, another XBM subsystem name, or an MVS command.

- You can use a single PROC for multiple subsystems if you want to use XBM in a data sharing environment and you use the `&SYSCLONE` symbolic from MVS system symbols. For more information, see “Defining PROCs for use with multiple XBM subsystems” on page 286.

- You can use the same XBM SSID on multiple XBM subsystems in a non-data sharing environment.

XBM uses systems-wide enqueues in order to add an extra layer of protection for the XBM repository and to provide data sharing capability. If you do not intend to use XBM in a data sharing environment with shared repositories, you can use the same XBM ID on each LPAR/JES SSID. To do so, you must update the GRSRNLxx member in SYS1.PARMLIB and correctly modify the SYSTEMS EXCLUSION LIST.

Any resource named in this list is treated as a local resource when an ENQ, DEQ, or RESERVE macro is issued for the resource and is specified with a scope of SYSTEMS.

If you are not running with shared repositories, you must ensure that each repository has unique names to avoid ENQ conflicts.

You can use the `&SYSNAME` parameter (D SYMBOLS) to differentiate the repository from a single PROC. For example, after you use IDCAMS to define the data sets for your XBM started tasks, use the following example in the PROC to allocate the different repository on each LPAR.

```c
//XBMREP01 DD DISP=SHR,DSN=HLQ.XBM..SYSNAME..XBMREP01
```
Assume that you have an XBM SSID of XBMP. You would update the SYSTEMS EXCLUSION LIST in SYS1.PARMLIB(GRSRNLxx) with the QNAME of BMCXBM, the RNAME value of XBMP, and the TYPE value of SPECIFIC, as follows:

```
RNLDEF RNL(EXCL) TYPE(SPECIFIC)
  QNAME(BMCXBM)
  RNAME(XBMP)
```

You can use TYPE(SPECIFIC) only for a 4-byte XBM SSID.

If you have a 3-byte SSID name (for example, XBM), use a generic resource name entry to match a portion of a resource name. A match occurs whenever the specified portion of the generic resource name entry matches the beginning of the same portion of an input search argument.

```
RNLDEF RNL(EXCL) TYPE(GENERIC)
  QNAME(BMCXBM)
  RNAME(XBM)
```

You can dynamically activate the updated RNL by using the SET GRSRNL=xx IBM z/OS operator command. You must restart any active XBM subsystems to pick up the change.

To show all resources for the BMCXBM major QNAME, issue the following DISPLAY command:

```
D GRS,RES=(BMCXBM,*)
```

---

**Example**

**WARNING**

The SYS parameter on the started task JCL (or on the XBM START command) names the XBM subsystem only. Do not use any MVS subsystem name, DB2 subsystem name, or MVS subsystem command for the SYS parameter.

XDB2, XIMS, XVSAM, XSSI, XPSS, XZIIP

These parameters specify whether the indicated component will start when the XBM subsystem starts.

By default, all components with a valid password start when you start the XBM subsystem the first time. Upon subsequent starts of the XBM subsystem, XBM components will try to resume the state that they were in when the XBM subsystem stopped. Authorized components that were running will restart, but components that were stopped or disabled will not start. If you do not want a component to start, specify N or NO for the corresponding parameter value.

For example, if you do not want the SSI component to start, enter XSSI='NO' as a parameter for the PROC. If you want to restart the component later, you can use the XBM ISPF interface or the START console command.
Note
If you are using SUF and are not planning to use hardware snapshots or Instant Snapshots, BMC recommends that you specify not to start the SSI component. Doing so bypasses the device discovery phase and reduces startup times.

DD statements

The start procedure includes DD statements that you should define.

Table 111 on page 285 describes the DD statements.

Table 111: DD statements for XBM started task

<table>
<thead>
<tr>
<th>DD statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XBMREPPn</td>
<td>This statement is required. It references the XBM repository data sets. The suffix \textit{nn} represents a number from 01 through 09. If you allocate multiple repository data sets, the number suffixes must be sequential and begin with 01. In the sample JCL for an XBM started task in “Defining and starting the XBM started task” on page 280, two repository data sets are allocated.</td>
</tr>
<tr>
<td>BMCPSWD</td>
<td>This optional statement specifies the location of the XBM authorization modules. At initialization, XBM attempts to find authorization modules in the BMCPSWD DD statement, or if BMCPSWD library is not used, within the XBM STEPLIB or linklist. If XBM cannot find the authorization modules, XBM component activation fails. \textbf{Note:} If you specify both the BMCPSWD statement in the PROC and include authorization modules within your STEPLIB or linklist, XBM uses only the authorization modules specified in the BMCPSWD statement to authorize the product.</td>
</tr>
<tr>
<td>PROIGN</td>
<td>This statement is required when using XBM and FlashCopy version 2 to process snapshots in the same environment as the BMC MainView SRM product. This statement prevents MainView SRM from changing the snapshot allocations. If you use another product to manage volume allocation or volume pooling, see that product’s documentation for information about how to exclude XBM from that management.</td>
</tr>
<tr>
<td>X37IGN</td>
<td>This statement protects XBM from STOPX37 processing.</td>
</tr>
<tr>
<td>XBMXINIT</td>
<td>This optional statement points to an XBM initialization command file. This command file allows you to specify commands for XBM to perform automatically during initialization.</td>
</tr>
</tbody>
</table>
BMC recommends that you specify REGION=0M, which allows XBM to dynamically obtain enough storage to allocate its internal structures. If XBM does not have the storage necessary to create internal structures, initialization fails. If you use IEFUSI exits to limit region size, specify a minimum REGION=65M to allow XBM enough storage to allocate its internal structures.

---

**Defining PROCs for use with multiple XBM subsystems**

Use the following procedure to set up multiple XBM subsystems.

1. Use the Installation System to unload the XBM libraries to a common XBM load library.

2. On each system where you want to run XBM, create an XBM PROC that points to the common XBM load library.

---

**Note**

XBM repositories can be shared among XBM subsystems. However, to create unique repositories for each XBM subsystem, run the $230VSAM job and provide a different data set name for the repository on each XBM subsystem.

As an alternative to creating multiple PROCs, you can also use one of the following methods to enable the use of a single PROC to start multiple XBM subsystems:

- Override the SYS parameter to a unique XBM SSID when you issue the START XBM command. For example, issue
  - `START XBM,SYS=XBM1` to start the XBM subsystem on SYS1
  - `START XBM,SYS=XBM2` to start the XBM subsystem on SYS2
  and so on.

- Use the `&SYSCLONE` symbolic from the MVS system symbols as part of the SYS parameter.
  Using `&SYSCLONE` allows you to create unique XBM SSIDs across the sysplex without having separate PROCs. You can create two-, three-, or four-character IDs by combining `&SYSCLONE` with other literal characters. Table 112 on page 287 provides examples of using `&SYSCLONE` with other characters to produce unique identifiers.
### Table 112: Using &SYSCLONE in the SYS parameter

<table>
<thead>
<tr>
<th>Specification</th>
<th>Results</th>
<th>Examples</th>
</tr>
</thead>
</table>
| SYS=&SYSCLONE       | Two-character, unique subsystem identifier| — Subsystem SYSO: XBMSSID=SO  
|                     |                                          | — Subsystem SYSP: XBMSSID=SP                                              |
| SYS= A &SYSCLONE    | Three-character, unique subsystem identifier| — Subsystem SYSO: XBMSSID=ASO  
|                     |                                          | — Subsystem SYSP: XBMSSID=ASP                                              |
| SYS= XB &SYSCLONE   | Four-character, unique system identifier  | — Subsystem SYSO: XBMSSID=XBSO  
|                     |                                          | — Subsystem SYSP: XBMSSID=XBSP                                              |
| SYS= AH &SYSCLONE   | Four-character, unique system identifier  | — Subsystem SYSO: XBMSSID=AHSO  
|                     |                                          | — Subsystem SYSP: XBMSSID=AHSP                                              |

To determine the value of &SYSCLONE at your site, contact your system programmer.

### Customizing XBM$OPTS for data sharing environments

If you are using XBM in a data sharing environment, BMC recommends that you specify a pattern mask in the XBMSSID parameter of the XBM$OPTS member.

Doing so allows you to use the ISPF interface to access all XBM subsystems that match the pattern using a single CLIST and XBM$OPTS member. Otherwise, you would need a different XBM$OPTS member for each XBM subsystem.

For example, if you name your XBM subsystems XBMA, XBMB, and XBMC, you can specify the pattern XBM* as the value for XBMSSID in the XBM$OPTS member. This value enables you to access all of these subsystems. For an example of the XBM$OPTS member, see Figure 41 on page 287.

**Figure 41: Sample of XBM$OPTS member**

```rexx
/* REXX */  
/* XBM(TM) VERSION 6.1.XX */  
XBMSSID = 'XBM*'  /* XBM SUBSYSTEM ID */  
XBMLLIB = 'HLQ.XXLINK'  
XBLOAD = 'HLQ.XXLINK'  
XBMLIB = 'HLQ.XXPLIB'  
XBMTLIB = 'HLQ.XXPLIB'  
ADDRESS ISPEXEC "VPUT (XBMSSID) SHARED"
```
Where to go from here

Depending on the XBM components you plan to use, you might need to perform additional tasks to customize the components. See the chapter about customizing and managing the XBM subsystem in the *EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE User Guide*.

Using the XBM initialization command file

The XBM initialization command file allows you to specify commands for XBM to perform automatically following initialization.

For example, you can instruct XBM to activate several management sets after initialization.

The XBMXINIT DD statement that is included in the XBM PROC points to the command file. The command file is a data set you create that lists the commands that you want to execute. Figure 42 on page 288 shows an example of an XBM initialization command file.

**Figure 42: XBM initialization command file**

```plaintext
* *****XBM INITIALIZATION COMMAND FILE*****
* COMMAND TO ACTIVATE MANAGEMENT SETS
ACT MS PRODUCTION_1
* ************************************************
```

The command file in Figure 42 on page 288 supports the comment operator command, "* " (asterisk followed by a space). You can include the comment command in the file to provide descriptive text. Comments are echoed to SYSPRINT and the MVS console.

**Note**

BMC does not recommend activating a configuration by using the initialization command file. If you do not specify a configuration in the PROC, XBM automatically activates the last configuration that was used before it starts to process the initialization command file. If you then activate a configuration in the command file, XBM must deactivate the configuration it started with the PROC before activating the new configuration.
Customizing XBM components

This section provides a brief overview of the optional components that you might need to set up before using XBM:

- If you are planning on performing hardware or Instant Snapshots, you must set up the SSI component. This component manages communication between XBM and the hardware devices.

- If you are going to use XBM for snapshot processing in a DB2 or IMS data sharing environment, you must set up the PSS component.

For more information about these tasks, see the EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE User Guide.

Setting up the SSI component

The SSI component, when used with supported software and hardware, can perform hardware-assisted snapshot processing and Instant Snapshots.

This section explains how to install and configure the software and hardware products that the SSI component requires.

Before you begin

Contact your intelligent storage vendor to ensure that the software for your devices has appropriate PTFs and microcode installed to support XBM hardware-assisted snapshot functions.

When you start the SSI component, XBM starts a discovery process that locates and determines the status of supported storage devices that you have in your environment. Through the SSI monitor, you can view and manage these devices. The amount of time it takes XBM to perform the discovery process depends on the number and complexity of hardware devices in your environment.

To set up the SSI component

1. Install one of the storage devices and the appropriate supporting software that are listed in Table 113 on page 289.

Table 113: Hardware and software requirements for SSI

<table>
<thead>
<tr>
<th>Storage device</th>
<th>Required software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic device capable of PPRC</td>
<td>Version of MVS that supports PPRC operations</td>
</tr>
</tbody>
</table>
### Storage device

<table>
<thead>
<tr>
<th>Storage device</th>
<th>Required software</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC Symmetrix a</td>
<td>■ EMC Symmetrix Control Facility b (SCF) subsystem</td>
</tr>
<tr>
<td></td>
<td>■ EMC TimeFinder c</td>
</tr>
<tr>
<td>Hitachi ShadowImage</td>
<td>■ Version of MVS that supports PPRC operations</td>
</tr>
<tr>
<td></td>
<td>■ Remote Copy (HRC)</td>
</tr>
<tr>
<td></td>
<td>■ IBM DFSMS/MVS Remote Copy Support</td>
</tr>
<tr>
<td>IBM Enterprise Storage Subsystem (Shark)</td>
<td>■ IBM FlashCopy version 2</td>
</tr>
</tbody>
</table>

**a** To use the volume-level snapshot method, you must install the 5x63 level of EMC microcode. If you plan to use the data set-level or Instant Snapshot method, you must install the 5x66 level of EMC microcode.

**b** To use the SCF subsystem, you must reference the location of the subsystem in the XBM STEPLIB or in the MVS link list.

**c** If you have EMC TimeFinder version 5.3.1 or later, you might need two EMC products. If you are performing mirroring, you will need EMC TimeFinder/Mirror. If you are performing data-set-level or Instant Snapshots, you will need EMC TimeFinder/Snap. EMC separated the mirroring and SNAP capability in EMC TimeFinder version 5.3.1. For more information, see the EMC documentation.

---

2 Configure the XBM product, including the SSI component.

For more information about configuring the SSI component, see *EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE User Guide*.

---

### Setting up the PSS component

The PSS component enables snapshot utilities processing in a DB2 sysplex (data sharing) environment and snapshot processing in an IMS data sharing environment.

To use the PSS component, perform the steps described in this procedure.

1 Add the XBM cache and list structures to your coupling facility resource manager (CFRM) policy.
For detailed information about these CFRM structures, see the *EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE User Guide*.

**Note**
A single set of XBM structures in the CFRM policy is valid for multiple DB2 data sharing groups.

2 Install and initialize an XBM subsystem on each CPU running DB2 or IMS in the sysplex.

**Note**
All XBM subsystems in a data sharing group should be the same version.

3 Specify the appropriate values on the PSS Options panel.

Instructions for accessing the PSS Options panel and setting appropriate values can be found in the *EXTENDED BUFFER MANAGER and SNAPSHOT UPGRADE FEATURE User Guide*.

4 Stop and restart the PSS component on each XBM subsystem to enable the options.
Customizing BMC Workbench

After you install the BMC Workbench for DB2 product, you might need to perform several additional customization tasks to complete and verify the installation. You perform these tasks outside the Installation System.

Customization overview

This section provides an overview of the component architecture, procedure, and requirements of the customization process of BMC Workbench.

Architecture of BMC Workbench

BMC Workbench for DB2 uses common BMC infrastructure components:

If they were not already installed for other BMC products, installing BMC Workbench also installs the following components:

- UIM - started task for User Interface Middleware. A minimum of one UIM is required for each SYSPLEX.

- DBC - started task for BMC DB2 Component Services. One DBC is required for each LPAR where BMC Workbench is installed.

- LGC - a DB2 Product Configuration agent that runs within the DBC. One LGC is required for each DBC started task.

- RTCS - started task for Runtime Component Services. One RTCS is required for each LPAR where BMC Workbench is installed.

Infrastructure operation

The following process summarizes how the infrastructure components help control the product's operation:
1. You enter your BMC Workbench URL in your web browser and provide your logon credentials.

2. You are signed on to the UIM, which matches the host and port from the URL.

3. When you request information from a DB2 subsystem, the UIM contacts the local DBC that is running the GUDWBNCH namespace.

4. The DBC contacts other DBCs in the same DBC Group to return a list of DB2 subsystems that are available to you as a BMC Workbench user.

**DBC agents**

The BMC Workbench client uses multiple agents that run under the control of a DBC to provide DB2 related information. Each agent (Navigation, DDL, Execution, and Explain) is responsible for specific information requests from the BMC Workbench client:

- The Navigation agent (GUD) processes all requests related to DB2 catalog objects, such as generating a list of tables.

- The DDL agent (DDL) processes all requests related to generating SQL or DB2 command syntax, such as CREATE, DROP, START, STOP, DISPLAY, and BIND.

- The Execution agent (EXE) processes all DDL, DML, DB2 command, and MVS job submission requests, such as processing the SQL syntax that the DDL agent generated.

- The Explain agent (EXP) is responsible for processing all requests related to SQL tuning, such as accessing information in the DB2 SQL cache or performing an Explain of an SQL statement.

The agents run as a service within the DBC. As such, multiple instances of each agent can be active at any given time, based on the configuration parameters that are set up in the DBC. For more information, see the *BMC Infrastructure Components Administration Guide*.

**BMC Workbench for DB2 requirements**

BMC Workbench for DB2 has the following requirements:

- BMC Workbench version 12.1 requires that you install CATALOG MANAGER version 12.1.
Note
If you do not have a license for CATALOG MANAGER, the required CATALOG MANAGER infrastructure is installed together with BMC Workbench.

- Configure a TSO region size of 32 MB or greater for each user who signs on.
- The default value of the z/OS Workload Manager (WLM) environment name must match the name of the WLM address space (with a maximum of eight characters).
- To successfully execute the DB2 commands (BIND, REBIND, FREE, START, STOP, DISPLAY), you must have the IBM supplied stored procedure, SYSPROC.ADMIN_COMMAND_DSN, installed and the Workload Manager (WLM) defined.

In addition, ensure that the following dd statement is defined in your WLM startup JCL:

```bash
//SYSEXEC DD DISP=SHR, DSN=db2ClistDataset
```

- Each started task requires a user-selected subsystem ID. These subsystem IDs must not be predefined to the operating system (for example, they should not be defined in IEFSSNxx members in SYS1.PARMLIB, nor by the SETSSI ADD command). If you redefine the subsystem ID, an IPL might be required to upgrade to a new release or maintenance level.
- If you are using a security package such as IBM RACF or CA Technologies CA-ACF2 or CA-Top Secret, the System Authorization Facility (SAF) must be enabled.
- The dispatching priority of the BMC DB2 Component Services (DBC) technology should be higher than that of the DB2MSTR and DB2DBM1 regions.
- You can run the DBC as a batch job or as a started task. The job or started task must have a user ID (also referred to as a LOGON ID or ACID) associated with it. If you run the DBC as a started task, assigning a user ID might involve system updates or security table updates.
- BMC does not recommend running the DBC in batch mode unless you are testing the initial installation. Stopping products that are running in batch mode terminates the initiators in which the products are running.
- Define at least one superuser for your BMC Workbench installation.
- DB2 Component Services (DBC)

BMC Workbench uses GUD agents that require the DB2 DSNLOAD library. Unless that library is already included in your LINKLIST, you must add the DB2
DSNLOAD library to the <LOADLIB> tags in the GUDINIT step of the $480INIT job.

For more information, see Knowledge Article 000103857 on BMC Support Central.

- If there are multiple BMC Workbench installations sharing a single repository:
  - There must be only one UIM HFS dataset per repository. If multiple UIMs share a repository, then they must also share the UIM HFS dataset.
  - All BMC Workbench installations must have the same maintenance level (same PTFs).

### Installing SYSPROC.ADMIN_COMMAND_DSN

If you have not yet installed SYSPROC.ADMIN_COMMAND_DSN complete these steps:

1. Create a JCL startup procedure for the IBM z/OS Workload Manager (WLM) environment.

2. Create the SYSPROC.ADMIN_COMMAND_DSN stored procedure in the DB2 catalog, and specify the WLM environment.

3. Activate the WLM environment.

   **Note**

   For more information, see the *IBM DB2 for z/OS Installation Guide*.

### Creating the superuser SAF resource

Each BMC Workbench installation must have at least one superuser. Complete the following procedure only if you want to use the user-access feature and did not previously use `ACT.WBSU.%HOST%.%PORT%` to define a superuser.

**Note**

*Information for ACF2 users*

To create a superuser or to manage user-access to BMC Workbench functions, define the resource as `TYPE(XFC)` where the documentation refers to the RACFXFACILIT class.

1. Verify that the User Interface Middleware Server (UIM) PTF BPJ0835 has been installed.
2 For each UIM installation, create the following SAF resource as a XFACILIT class: BMCGUD.WBSU.%SYSNAME%.%PORT%.
Replace the variables %SYSNAME% and %PORT% with the MVS system name and port number on the UIM server.

Note
The MVS system name is the value of the SYSNAME system symbol and can be obtained using the MVS system command D SYMBOLS.

3 Assign ALTER authority to the superuser resource for the user requiring superuser authorization on that UIM.

Selecting a subsystem for the BMC Workbench repository

Product information, such as user preferences and workspaces, is saved in a repository on a DB2 subsystem.

Only BMC Workbench superusers can select the DB2 subsystem where the repository is installed.

Tip
After you have stored user preferences and workspaces, BMC recommends that you do not change where the repository is installed. If you have to change your repository, contact BMC Support for advice.

Note
Consider the following guidelines if you have BMC Workbench installations sharing a single repository:

- You should have only one UIM HFS data set per repository. If multiple UIMs share a repository, they must also share the UIM HFS data set.
- All BMC Workbench installations must have the same maintenance level (that is, the same PTFs applied).

To select the subsystem

1 On the browser's main menu bar, click Tools => Server Setup.
2 Select Workbench Repository.
3 Select a DB2 subsystem and click OK.
Editing the BMC Workbench option set

The BMC Workbench for DB2 product options, known as GUDOPT option sets, provide default values that control the product’s behavior during execution.

The installation process automatically creates a default option set named GUDOPT that is based on definitions that you supply during installation.

Note
For more information, see the section explaining how to work with option sets in the BMC Infrastructure Components Administration Guide.

For each GUDOPT option set, you can specify the following details:

- Specify the plan that various components of BMC Workbench use when accessing IBM DB2 resources.
- Specify the product default options module that Catalog Access component uses. For more information, see Step 6 on page 299.
- Specify the name of the PDS that contains the product XML configuration member. For more information, see Step 6 on page 299.
- Specify the name of the PDS that contains the ISPF MLIB-like members used by the product. You can specify up to three data sets. If you specify more than one data set, the data sets are concatenated for use in the order specified. For more information, see Step 7 on page 299.
- Specify the Run authorized option. This option enables you, if your user ID does not have explain authority, to allow explain to acquire SYSADM authority before doing the explain. The default is N. For more information, see Step 7 on page 299.
- Specify the rules engine data set that contains the processing rules for the SQL Tuning component. For more information, see Step 7 on page 299.

To edit a GUDOPT option set

Note
Any changes that you make to the BMC Workbench option set (GUDOPT) affect all users.

1 Invoke the LGCISPF CLIST from the CLIB data set:
   EX 'HLQ..BMCCCLIB(LGCISPF)'
If you want to connect to a DBC other than the default DBC, invoke the CLIST with the DBC parm where xxxx is the DBC SSID on that LPAR:

**EX 'HLQ..BMCCLIB(LGCISPF)' 'DBC(xxxx)'**

2 In the DB2 Product Configuration - Main Menu (panel LGCPMENU), select 2 Manage Product Options.

3 In the Product Options Sets panel (LGCP1001) expand the BMC Workbench list by selecting the plus sign (+) next to BMC Workbench and pressing **Enter**.

4 Type **E** next to the option set that you want to edit.

5 For Common Options DB2 Plan Name, specify your BMC Workbench plan.

---

**Note**
The default plan name is BMCGUIPL.

---

6 At **Catalog Access Options**, specify the following values:

- At **Product DOPT Name**, specify the product default options module (DOPT) that the Catalog Access component uses.

- At **Configuration DSN**, specify the data set that contains the product XML configuration member.

- At **Message DSN #1-3**, specify the Catalog Manager MLIB data set that contains the ISPF MLIB members used by the product. You must specify the message DSN #1.

7 At **SQL Tuning Options**, specify the following values:

- At **Run authorized - N/Y**, you can allow explain to acquire SYSADM authority before doing the explain if your user ID does not have explain authority. The default is **N**.

- At **Rules DSN**, you specify the SAMP data set used by common explain that contains the processing rules for the SQL Tuning component.

8 Press **F3** to exit and save.

A validation process checks your entries. If any validation errors exist the cursor is positioned on the Filter: Invalid View screen.

For more information about correcting validation errors, see the *BMC Infrastructure Components Administration Guide*.  

---

Chapter 9 Customizing BMC Workbench 299
To have your changes take effect, stop and restart the GUD agents in the DBC by issuing the following commands in SDSF:

- `/dbcssid GUD,STOPALL`
- `/dbcssid GUD,STARTALL`

## Common Explain

The Common Explain technology enables you to Explain dynamic and static SQL statements. Common Explain provides both statistical and textual information about the access path, and suggests how to improve SQL statement performance.

## Expert rules

The Explain feature is driven by a set of expert rules.

These rules trigger messages that tell you where performance problems exist and what design changes are needed. Each expert rule has an associated severity value and threshold.

## Severity codes in rules

Each message that is associated with a rule has a severity code.

The severity code determines the order in which the messages are displayed and the color used to display them. Severe messages are displayed first, followed by warning and informational messages.

The severity code is displayed as the tenth character in the message identifier (as shown in the following example).

**Example**

BMC184032W

Table 114 on page 301 shows the possible severity codes.
Table 114: Severity codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>S (severe error)</td>
<td>Correct the issue before continuing.</td>
</tr>
<tr>
<td>W (warning)</td>
<td>Review the messages before continuing, to determine whether you need to correct the issue.</td>
</tr>
<tr>
<td>I (informational)</td>
<td>The message provides additional information, but no action is required.</td>
</tr>
<tr>
<td>X (suppress)</td>
<td>The message is suppressed (not displayed).</td>
</tr>
</tbody>
</table>

Using predefined rules

The product includes predefined sets of rules, intended for different groups of users. The rules files are available in the HLQ.BMCSAMP data set.

**To select predefined rules**

1. In BMC Workbench, on the SQL Tuning Options dialog box, select the rule set (DEFAULT or APPLDEV) that you require from the list.

Defining new expert rules

You can define new expert rules variables (facts) by creating a REXX EXEC. Common Explain creates the set of rules variables based on the SQL statement that is being explained. You can set new values for those variables and you can make your own variables.

**To define new expert rules**

1. Using a text editor, create a REXX exec.

   **Note**
   
   The BMCSAMP data set contains a sample REXX exec (PSSREXI) that you can edit to create a customized rule set.

2. Save the edited REXX exec as a member of the same data set as the rule sets.

   The name of the member must be PSSREXIT.
If PSSREXIT exists in the data set, Common Explain executes the REXX exec before running the rules engine. The REXX exec replaces and adds variable values to which the rules engine will subsequently refer.

REXX exec can call the following functions:

- **SETS and SETF functions** take two arguments, the variable name and the variable value.
- **GETS and GETF functions** take one argument, the variable name.
- **PSSRXSQL function** takes one argument, an SQL statement.

By calling the PSSRXSQL function, the REXX exec can perform the following SQL statements:

- FETCH INTO
- SELECT INTO
- COMMIT
- ROLLBACK
- OPEN
- CLOSE
- EXECUTE IMMEDIATE (for executing INSERT, UPDATE, or DELETE SQL statements)

PSSRXSQL sets the following REXX variables after executing an SQL statement:

- SQLCODE
- SQLSTATE
- SQLERRM (contains the text of an error message)
- “INTO” variables
- cursor_name.n variables

For more information, see “PSSRXSQL external function” on page 304.

### Structure of rules

You store rules in a data set member.

The rules are stored in the BMCSAMP data set, in the following members:

- PSSDFLT for default rules
- PSSAPPL for rules for application developers
- PSSJAPAN for rules in Japanese
Standard format for a rule set

The first line of the data set member contains the rule set declaration:

```
RULESET ruleSetName
```

Following the RULESET declaration, you can have one or more rules. Rules are processed in the order in which they are defined in the rule set. Each rule adheres to the following standard format, though the ELSE clause is optional.

```
name: IF predicate
    THEN OUT=action1
    ELSE OUT=action2
```

In this format, the variables are as follows:

- `name` indicates the name of the rule and must be unique within the rule set. Do not include a space between the name of the rule and the colon.

- `predicate` is an IF statement that specifies the value that is being evaluated and the value to which it is being compared. The predicate can include multiple conditions separated by AND or OR.

  **Example**
  - IF UPDATE_NO_WHERE = "Y"
  - IF MIN = "Y" OR MAX = "Y"
  - IF OPTIMIZE = "Y" AND (MIN = "Y" OR MAX = "Y" OR AVG = "Y" OR SUM = "Y")
  - IF PARTITIONS > 0

- `action1` value indicates the action that is performed if the condition within the predicate is true. Usually, the action specifies issuing a message. The message must end with \n and be enclosed in quotes. Vertical bars (||) indicate that the message continues across lines.

  **Example**
  ```
  THEN OUT=OUT||"BMC184024I-Consider the use of BETWEEN in "||"
  place of > and <=. DB2 may consider using an index to provide the"||"
  answer.\n"
  ```

- `action2` indicates the action that is performed if the condition within the predicate is false. This value follows the same rules as `action1`.

Samples from the default rule set

Following are descriptions of sample rules (RULE1032, RULE2002, and RULE1026) from the default rule set.
RULE1032 triggers if OPTIMIZE and UNION are both used. The rule then produces a message that indicates that the rows will not be optimized due to this condition:

```
RULE1032: IF OPTIMIZE = "Y" AND UNION = "Y"
    THEN OUT=OUT||"BMC184032W-The OPTIMIZE FOR N ROWS will be ignored due to the use of a UNION, UNION ALL, or UNION DISTINCT."
```

RULE2002 triggers if VALIDATE is set to R. The rule then produces a message to indicate that this setting can impact performance:

```
RULE2002: IF VALIDATE = "R"
    THEN OUT=OUT||"BMC184172I-The SQL and DB2 authorizations will be checked at execution time. This can adversely impact performance. Review with DBA on this usage."
```

RULE1026 provides two different message outputs by providing an ELSE statement. If QUALIFIED is set to N, one message is generated; otherwise, a different message is generated.

```
RULE1026: IF QUALIFIED = "N"
    THEN OUT=OUT||"BMC184026I-The tables referenced in the FROM clause are not qualified. These will be resolved at bind time by the QUALIFIER name, by a SET CURRENT SQLID/SCHEMA if the query is dynamic, or it will default to the executing AUTH ID."
ELSE OUT=OUT||"BMC184028I-The tables referenced in the FROM clause are fully qualified. This will limit the flexibility for the qualifier to be resolved at bind time."
```

**PSSRXSQL external function**

The PSSRXSQL external function sets values according to the SQL statement. You can call PSSRXSQL from REXX exec whenever you need to execute SQL.

In each example in Table 115 on page 304, the argument in parentheses is an SQL statement. When PSSRXSQL runs, it sets the variable `rc` to the return code of the command that ran. The value in the `rc` variable determines subsequent processing. Using this external PSSRXSQL function, you can perform any SQL statement.

**Table 115: PSSRXSQL external function**

<table>
<thead>
<tr>
<th>SQL statement</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN CURSOR</td>
<td><code>rc = pssrxsql(&quot;OPEN cursorName CURSOR FOR&quot; sqlStatement)</code></td>
<td>Prepare the SQL SELECT statement and open the specified cursor.</td>
</tr>
<tr>
<td>FETCH CURSOR</td>
<td><code>rc = pssrxsql(&quot;FETCH cursorName&quot;)</code></td>
<td>Fetch the first or next row.</td>
</tr>
<tr>
<td></td>
<td><code>rc = pssrxsql(&quot;FETCH cursorName INTO v1, v2, ... vn&quot;)</code></td>
<td>Return SQLCODE = 100 when all rows have been fetched. The first form of the function puts the data into variables whose names are <code>cursorName.columnName</code>. It also puts values into variables like <code>cursorName.n</code>, where <code>n</code> is the column number of the query. The second form puts values into the specified variables. The maximum length of a variable name is 250 characters. Variable names can contain <code>@</code>, <code>#</code>, <code>$</code>, <code>¢</code>, <code>.</code>, <code>!</code>, <code>?</code>, or <code>_</code>.</td>
</tr>
<tr>
<td>SQL statement</td>
<td>Example</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CLOSE CURSOR</td>
<td>rc = pssrxsql(&quot;CLOSE cursorName&quot;)</td>
<td>Close the specified cursor.</td>
</tr>
<tr>
<td>EXECUTE</td>
<td>rc = pssrxsql(sqlStatement)</td>
<td>Prepare and run the SQL statement.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the statement is SELECT, return no more than one row. The function sets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>variables as it does for FETCH. If the SELECT statement has no INTO clause,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the stem name is always SELECT.</td>
</tr>
<tr>
<td>COMMIT</td>
<td>rc = pssrxsql(&quot;COMMIT&quot;)</td>
<td>Commit uncommitted work, and close all open cursors.</td>
</tr>
<tr>
<td>ROLLBACK</td>
<td>rc = pssrxsql(&quot;ROLLBACK&quot;)</td>
<td>Back out relational database changes made since the last commit.</td>
</tr>
</tbody>
</table>

**Note**

The current version of the PSSRXSQL external function does not support the following items:

- More than three open cursors at the same time
- Parameter markers
- The DESCRIBE command
- Mixed-case commands
- LOBs

Commands must be all lowercase or all uppercase. For example, either open or OPEN is acceptable, but oPeN is not valid.

**PSSRXSQL return codes**

If PSSRXSQL encounters non-SQL errors, it returns one of the following return codes:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Success</td>
</tr>
<tr>
<td>30</td>
<td>No command in the argument string</td>
</tr>
<tr>
<td>31</td>
<td>Already disconnected</td>
</tr>
<tr>
<td>32</td>
<td>Already connected</td>
</tr>
<tr>
<td>33</td>
<td>Cursor already open</td>
</tr>
<tr>
<td>34</td>
<td>Too many open cursors</td>
</tr>
<tr>
<td>Return code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>35</td>
<td>Unknown cursor</td>
</tr>
<tr>
<td>36</td>
<td>Out of memory</td>
</tr>
</tbody>
</table>
| 37          | SQL failure  
The variable SQLCODE is set, and the variable SQLERRM contains a printable error message. |
| 38          | Argument string length greater than 32,767 characters |
| 39          | An ‘INTO’ was expected but not found |

### Printing error messages

The following code formats and prints SQL error messages to the SYSTSPRT data set when the product is running in batch mode or TSO:

```plaintext
rc = pssrxsql("select current_timestamp into :TS from sysibm.sysdummy1")
if rc <> 0 then do
    msg = "BMC184001S-PSSREXIT rc=" || rc || "\n"
    if sqlcode <> 0 then do
        m = substr(sqlerrm, i + 1, 79)
        if m = '' then leave
        msg = msg || "BMC184001S-" || m || "\n"
    end
    rc = sets("OUT", msg)
end
```

**Note**

BMC does not recommend using the SAY command instead of the STEPS function because the DBC does not allocate a SYSTSPRT data set.

You can use the REXX variable SQLSTATE instead of SQLCODE. SQLSTATE indicates both warnings and errors.

If the product issues a warning without an error, PSSRXSQL returns `rc=0`, `SQLCODE=0`, ignoring warnings so that all the row values are returned. If you want to inspect warnings, use the SQLSTATE variable.
Customizing NGT utilities

After you install any NGT utilities, you might need to perform several additional customization tasks to complete and verify the installation. You perform these tasks outside the Installation System.

Checkpoint data set considerations

For each subsystem, the installation process creates an NGTCKPT data set named UserHLQ.SSID.CKPT001.

WARNING
Do not place this data set under control of any compression or DASD management software package, as interference causes processing problems.

Consider the following points:

- You cannot copy a checkpoint data set, although you can dump it and restore it. Attempts to copy the checkpoint data set result in a user abend code of U0008.

- If the NGTCKPT data set UserHLQ.SSID.CKPT001 fills up, NGT automatically allocates a HLQ.CKPT002 data set to prevent failures. It is important to keep this CKPT0001 low level qualifier when you create your checkpoint data set in the $725ALOC installation job.

- BMC recommends that you avoid redefining the checkpoint data set. Redefining the checkpoint data set causes loss of common data that BMC Next Generation Technology (NGT) utility products use. If you need to redefine the checkpoint data set, either stop all NGT utility jobs or schedule the redefinition when no NGT utility jobs are active.

  Note
  Call BMC Customer Support before you redefine the checkpoint data set.

- BMC recommends that you reorganize the checkpoint periodically. For more information, see the chapter on checkpoint maintenance in the BMC Next Generation Technology General User Guide.
Place the checkpoint data on a DASD volume that is backed up daily.

Run the NGTDISP command regularly, and run QUICKEXIT for the specified UID to clean up any failed jobs that have RESTARTABLE or MUST COMPLETE status. Adjust the value of the +OUTPUTAGE parameter to reduce the time that completed jobs remain in the checkpoint data set. For more information, see the BMC Next Generation Technology General User Guide.

Block size considerations

The minimum block size is 4096. Generally, the larger the block size the better the performance of loading NGT utility products before execution. Since this occurs only once per utility step, the block size is a not a major consideration unless you use a small block size such as 6144.

In this case, for certain utility functions against small DB2 spaces (e.g. copying a table space of less than 10 cylinders) a disproportionate number of Execute Channel Programs (EXCPs) reported is attributable to program fetch activity.

Starting NGT Subsystem

Use the following procedure to start NGT Subsystem.

1. Issue the following operator command:

   $ CDBSS

   When NGT Subsystem is fully initialized, it issues message NGTC199 to the console.

   **Tip**

   BMC recommends that you place this start command in member COMMNDXX of SYS1.PARMLIB so that NGT Subsystem automatically starts during the IPL process.

   If you are using data sharing, you must start the CBDSS on all LPARs where any member of the DB2 group might be started.
Customizing the User Interface Middleware (UIM)

This chapter describes the customization tasks that should be performed after installation.

Starting and stopping the UIM server

To start and stop the UIM server, you must issue MVS operator commands on the host that the UIM server is installed on.

To start the UIM server

1. Issue the following MVS operator command, where `uimServerName` is the name of the UIM server started task:

   `/S uimServerName`

To stop the UIM server

1. Issue the following MVS operator command, where `uimServerName` is the name of the UIM server started task:

   `/P uimServerName`

   **Note**

   To avoid data loss, notify active users if you must stop the UIM server.

Changing UIM server options

If you modify any of the values in a $730DOPT job after configuration, you must use the following procedure to apply the changes.
The UIM server is configured during installation. However, you can view or alter the original configuration of the UIM server permanently by changing the values for variables in the startup and trace members of the configuration file.

You can change the following UIM server configuration options:

- **Port number**
  See “To change the port number” on page 310.
- **Authorization security timeout**
  See “To change the security authorization timeout feature permanently” on page 311.
- **Affinity timeout**
  See “To change the idle timeout for affinity tasks” on page 312.
- **Server-side storage (HFS) data set**
  See “To change the HFS server-side storage data set name” on page 312.
- **Tracing**
  See “To change the overall tracing option permanently” on page 313.
- **Enable/disable network browser command interface**
  See “To enable or disable the network browser command interface” on page 313.

Each UIM server requires a configuration member, called the startup member, that describes the unique characteristics of that server. This member is specified as a parameter in the UIM server configuration file.

The sample library contains a template for the startup member named #NORMAL. The installation process customizes the #NORMAL member, gives it the same name as the started task procedure, and copies it to the HLQ.XXCNFG data set.

For an example of this startup member and a description of the variables that you can change, see “Creating additional UIM servers” on page 316

### To change the port number

1. Edit your startup configuration member.

   A port number for the UIM server is the address of a TCP/IP application, in this case the UIM server, on a z/OS image. The UIM server has one port number that DASD MANAGER uses to contact the UIM server. You can change the port number globally for all applications that communicate with the UIM server.

   **Note**

   The startup member is located in the HLQ.UBMCCNFG data set and is typically the same name as the started task procedure name for the UIM server.
2 In your startup configuration member, find the PORT variable.

The default port number is 9999.

The PORT variable is displayed as follows:

```
<BMC_PARM ID="PORT"
VALUE="9999" />
```

3 Change the value of BMC_PARM ID="PORT" from 9999 to a unique numeric value between 1 and 65535.

**WARNING**

Check with your TCP/IP administrator to ensure that you are entering a unique port number. If you do not enter a unique port number, program errors might occur.

---

**To change the security authorization timeout feature permanently**

The UIM server is equipped with a timeout security feature. This feature controls the amount of time that all applications which communicate with the UIM server can remain inactive before security authorization expires. This value is set during installation. You can change the timeout feature permanently for all applications that communicate with the UIM server.

1 Edit your startup configuration member.

**Note**

The startup member is located in the HLQ.UBMCCNFG data set and is typically the same name as the started task procedure name for the UIM server.

2 From your startup configuration member, find the AFF_TIMEOUT_SECS variable.

The default number of seconds is 1800.

The AFF_TIMEOUT_SECS variable is displayed as follows:

```
<BMC_PARM ID="AFF_TIMEOUT_SECS"
VALUE="1800" />
```

3 Change the value of BMC_PARM ID="AFF_TIMEOUT_SECS" from 1800 to any numeric value in seconds.
To change the idle timeout for affinity tasks

Affinity timeout is the amount of time that the task is held between requests for the affinity. When the task is inactive for the defined period, the affinity is no longer valid and the task is available for other work.

1. Edit your startup configuration member.

   **Note**
   
   The startup member is located in the HLQ.UBMCCNFG data set and is typically the same name as the started task procedure name for the UIM server.

2. From your startup configuration member, find the AFF_TIMEOUT_SECS variable.

   The default number of seconds is 1800.

   The AFF_TIMEOUT_SECS variable is displayed as follows:

   ```
   <BMC_PARM   ID="AFF_TIMEOUT_SECS"
    VALUE="1800" />
   ```

3. Change the value of BMC_PARM ID="AFF_TIMEOUT_SECS" from 1800 to any numeric value in seconds.

To change the HFS server-side storage data set name

The server-side storage data set stores user preferences and dynamic configuration information on the UIM server.

1. Edit your startup configuration member.

   **Note**
   
   The startup member is located in the HLQ.UBMCCNFG data set and is typically the same name as the started task procedure name for the UIM server.

2. From your startup configuration member, find the HFS_DATASET variable.

   The HFS_DATASET variable contains the data set name to use for the UIM server server-side storage data set. The HFS_DATASET variable is displayed as follows:

   ```
   <BMC_PARM   ID="HFS_DATASET"
    VALUE="HLQ.HFS" />
   ```

3. Change the value of the high-level qualifier (HLQ) for HFS_DATASET to a value that meets your site’s standards.
To enable or disable the network browser command interface

The network browser command interface, also known as the BMC UIM server commands web page, displays UIM server information and allows an administrator to make dynamic modifications to UIM server settings.

You can enable or disable the network command interface. You can also provide an active authentication with the browse session. After the variable ALLOW_NETCMD is set to AUTH, the user must log in using the following command in the web browser:

```
http://uimServerHostName:uimPortNumber/UIMLogon
```

If the logon is successful, the user can display the BMC UIM server Commands web page (http://uimServerHostName:uimPortNumber/htpcmd.html).

1. Edit your startup configuration member.

   **Note**
   
   The startup member is located in the HLQ.UBMCCNFG data set and is typically the same name as the started task procedure name for the UIM server.

2. From your startup configuration member, find the ALLOW_NETCMD variable.

   By default, the network browser commands are processed by the UIM server, but you can disable them by setting the ALLOW_NETCMD value to NO.

   The ALLOW_NETCMD variable is displayed as follows:

   ```
   <BMC_PARM ID="ALLOW_NETCMD" VALUE="YES" />
   ```

3. Change the ALLOW_NETCMD value to one of the following values:
   - YES enables the network browsing command interface.
   - NO disables the network browsing command interface.
   - AUTH requires logging on via uimlogon.html.

To change the overall tracing option permanently

```xml
<BMCHTTP>
  <RRLOG VALUE="OFF"/>
  <TRACE VALUE="ON">
    <BMC_PARM ID="TRACE_ACTION" VALUE="TRACEACTION_WARNING" />
    <!-- BMC_PARM ID="TRACE_ACTION" VALUE="TRACEACTION_INFO" -->
    <!-- BMC_PARM ID="TRACE_ACTION" VALUE="TRACEACTION_ENTRYEXIT" -->
    <!-- BMC_PARM ID="TRACE_ACTION" VALUE="TRACEACTION_CONTROL" -->
    <BMC_PARM ID="TRACE_ACTION" />
  </TRACE>
</BMCHTTP>
```
1 Edit your trace configuration member.

The trace member is shown above.

2 From your trace configuration member, find the TRACE VALUE variable.

3 To enable or disable the overall tracing option, perform one of the following tasks:

   ■ To enable the overall tracing option, type ON inside the quotation marks, as shown in the following example:
     
     ```xml
     <TRACE VALUE="ON">
     ```

   ■ To disable the overall tracing option, type OFF inside the quotation marks, as shown in the following example:
     
     ```xml
     <TRACE VALUE="OFF">
     ```

4 Verify that the TRACE VALUE has been enabled or disabled.

**To verify that the overall tracing option is enabled**

1 Edit your trace configuration member.

2 Ensure that the overall trace option is enabled.

   If the overall trace option is enabled, the variable is displayed as follows:

     ```xml
     <TRACE VALUE="ON">
     ```
3 If the overall trace option is not enabled, edit the variable as required to enable it.

**To enable specific tracing options**

1 From the list of specific tracing options, find the option that you want to enable, as shown in the following example:

```xml
<!--BMC_PARM ID="TRACE_ACTION" VALUE="TRACEACTION_INFO" />
```

2 Remove the exclamation point, hyphens, and space (!--) that are displayed between the opening bracket (<) and text (BMC_PARM).

3 Remove the hyphens (-- ) that are displayed between the forward slash (/) and the closing bracket (>).

The specific tracing option is enabled, as shown in the following example:

```xml
<BMC_PARM ID="TRACE_ACTION" VALUE="TRACEACTION_INFO" />
```

**To disable specific tracing options**

1 From the list of specific tracing options, locate the option that you want to disable, as shown in the following example:

```xml
<BMC_PARM ID="TRACE_ACTION" VALUE="TRACEACTION_INFO" />
```

2 Type an exclamation point, two hyphens, and a space (!-- ) between the opening bracket (<) and text (BMC_PARM).

3 Type two hyphens (-- ) between the forward slash (/) and the closing bracket (>).

The specific tracing option is disabled, as shown in the following example:

```xml
<!--BMC_PARM ID="TRACE_ACTION" VALUE="TRACEACTION_INFO" />
```

## Accessing multiple z/OS systems

You must complete several tasks to access multiple z/OS system when you use Database Performance for DB2.

To access multiple z/OS systems, complete the following tasks:

- Create a UIM server on each system (see “Creating additional UIM servers” on page 316).
Creating additional UIM servers

You must have a separate UIM server for each z/OS system that you want to access. Use the procedures in this section to create additional UIM servers.

When the UIM server was installed, the sample startup procedure was copied, customized, and saved in your UIM sample library (HLQ.XXSAMP, where HLQ is the high-level qualifier that you specified during installation). Use this sample to create an additional UIM server.

To create a new UIM server, complete the following procedures in this section:

1. “To create a startup configuration member” on page 316
2. “To create a started task procedure” on page 317
3. “To allocate the HFS data set” on page 319
4. “To initialize the HFS data set” on page 320
5. “To enable or disable password caching” on page 321

To create a startup configuration member

1. Locate the #NORMAL member in the UIM sample library.

2. Create a new startup configuration member by copying the #NORMAL member from the sample library into your configuration file and giving it a new name.

You will use this same name when you name the started task procedure for the new UIM server. The following figure shows the startup configuration member. The HLQ shown in this member is the high-level qualifier that you specified during installation.

Figure 43: Startup configuration member

```xml
<BMCHTTP>
  <BMC_PARM ID="PORT" VALUE="9999" />
  <BMC_PARM ID="AUTH_TIMEOUT_SECS" VALUE="1800" />
  <BMC_PARM ID="AFF_TIMEOUT_SECS" VALUE="1800" />
  <BMC_PARM ID="HFS_DATASET" VALUE="HLQ.HFS" />
  <BMC_PARM ID="ALLOW_NETCMD"
```
3 Edit the new startup configuration member by changing the variables that are listed in the following table.

Table 117: Startup configuration member variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
<th>Accepted value</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;BMC_PARM ID=&quot;PORT&quot; VALUE=&quot;9999&quot;/&gt;</td>
<td>Port value for the UIM server</td>
<td>Unique numeric value in the range of 1 through 65535</td>
<td>Changing UIM server options on page 309</td>
</tr>
<tr>
<td>&lt;BMC_PARM ID=&quot;AUTH_TIMEOUT_SECS&quot; VALUE=&quot;1800&quot;/&gt;</td>
<td>Security authorization timeout</td>
<td>Numeric value in seconds</td>
<td></td>
</tr>
<tr>
<td>&lt;BMC_PARM ID=&quot;AFF_TIMEOUT_SECS&quot; VALUE=&quot;affinitySeconds&quot;/&gt;</td>
<td>Idle timeout period for affinity tasks</td>
<td>Unique numeric value in seconds</td>
<td></td>
</tr>
<tr>
<td>&lt;BMC_PARM ID=&quot;HFS_DATASET&quot; VALUE=&quot;HLQ.HFS&quot;/&gt;</td>
<td>Hierarchical file system (HFS) data set name</td>
<td>Extended partitioned data set (PDSE) name for storing the HFS data</td>
<td></td>
</tr>
<tr>
<td>&lt;BMC_PARM ID=&quot;ALLOW_NETCMD&quot; VALUE=&quot;YES&quot;/&gt;</td>
<td>Whether to enable or disable the network browser command interface</td>
<td>YES (default), NO, or AUTHORIZE</td>
<td></td>
</tr>
</tbody>
</table>

To create a started task procedure

After creating the startup configuration member, you must create a started task procedure for that startup member.

1 Locate the #UIMx member in the UIM server sample library.

2 Create a new #UIMx member by copying the #UIMx member to your system procedure library and giving the new member the name that you selected for the startup member.

The following figure shows the #UIMx member.

Figure 44: #UIMx member

```
//uimx     PROC M=uimx,            <-- name of configuration member
//             ENV=                  +
//*--------------------------------------------------------------
//uimx     EXEC PGM=UIMMAIN,                                           +
//             ACCT=(acct),        <--- specify accounting info        +
```
3 Edit the new #UIMx member.

   a Add your DB2 load library to the STEPLIB concatenation.
b Change the variables that are listed in the following table.

Table 118: #UIMx member data set name variables

<table>
<thead>
<tr>
<th>Data set name variables</th>
<th>Definition</th>
<th>Accepted value</th>
</tr>
</thead>
<tbody>
<tr>
<td>uimx</td>
<td>uimx is the name of the started task procedure and the startup configuration member</td>
<td>Name that you gave to the #UIMx member when you copied it to your system procedure library</td>
</tr>
<tr>
<td>HLQXXLINK</td>
<td>HLQ is the high-level qualifier for the load library that contains the UIM server and product execution code</td>
<td>Valid data set name qualifier</td>
</tr>
<tr>
<td>HLQ*LINK</td>
<td>HLQ is the high-level qualifier for the library that contains your product code</td>
<td></td>
</tr>
<tr>
<td>HLQXXCONT</td>
<td>HLQ is the high-level qualifier for the library that contains content information for the UIM server</td>
<td></td>
</tr>
<tr>
<td>HLQXXCNFG</td>
<td>HLQ is the high-level qualifier for the library that contains UIM server execution parameters that are used during initialization of the UIM server</td>
<td></td>
</tr>
<tr>
<td>HLQUIMCNFG</td>
<td>HLQ is the high-level qualifier for the library from the UIM configuration installation panel to write out tailored configuration members</td>
<td></td>
</tr>
</tbody>
</table>

**To allocate the HFS data set**

After creating the startup configuration member and the started task procedure, you can perform the following steps:

1. You can allocate and initialize the HFS data set.

   This server-side storage data set stores user preferences and dynamic configuration information on the UIM server.

2. You can submit the customized data set, or you can customize a copy of the data set member in the sample library.

   During installation, the HLQ.HFS member in the SAMP library was created and customized with your site specific information. You can submit the customized
data set, or you can customize a copy of the data set member in the sample library.

3 You can share the HFS data set between all UIM servers that are on the host, or you can create an HFS data set for each UIM that is on the host.

To customize a copy of the data set member

1 Locate the #DEFHFS member in the UIM sample library.

The following figure shows the #DEFHFS member. The HLQ shown in this member is the high-level qualifier that you specified during installation.

Figure 45: Default #DEFHFS member

```
//ALLPDSE EXEC PGM=IEFBR14
//HFSPDSE DD   DISP=(NEW,CATLG),UNIT=SYSDA,SPACE=(CYL,(1,1)),
//              DCB=(DSORG=PO,RECFM=VB,LRECL=4096),
//              DSNTYPE=LIBRARY,
//              DSN=HLQ.HFS
```

2 Edit the #DEFHFS member by changing the values of the parameters that are listed in the following table.

Table 119: #DEFHFS member information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
<th>Accepted value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIT</td>
<td>Device for placing data sets</td>
<td>See your site standards</td>
</tr>
<tr>
<td>DSN</td>
<td>High-level qualifier for the HFS data set</td>
<td>See your site standards</td>
</tr>
</tbody>
</table>

3 Save the edited #DEFHFS member with a new name.

4 Submit the DEFHFSJC member JCL.

To initialize the HFS data set

1 Before you can share connections in a sysplex, you must initialize the HFS data set that you allocated.

During installation, the HFSLOAD data set is created and customized with your site–specific information.

To submit a copy of the customized data set member

1 Locate #LOADHFS in the UIM server sample data set.
The following figure shows the default #LOADHFS member.

**Figure 46: Default #LOADHFS member**

```c
//--------------------------------------------------------------
//*
//*     Load the BMC HFS PDSE with SAMP library members.
//*     Optionally convert previous BMC HFS HostList.xml if found.
//*--------------------------------------------------------------
//LOADHFS EXEC PGM=UIMHFSL,REGION=0K,
//  PARM='=version $UIMHFSL $UIMHFST'
//*  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
//* UIMHFSL parameters:
//* memname Samplib control cards member, default is $HFSLOAD.
//* - $HFSLOAD is a Load of default properties files
//* -t Activate tracing to SYSPRINT
//* SAS/C Runtime Library parameters:
//* =version Print Runtime Library release information to SYSTERM
//*--------------------------------------------------------------
//STEPLIB DD DISP=SHR,DSN=HLQ.LOAD
//*
//* SAS/C DD'S
//SYSTERM DD SYSOUT=* 
//SYSPRINT DD SYSOUT=* 
//STGRPT DD SYSOUT=* 
//*
//* STANDARD JOB DD'S
//SYSUDUMP DD SYSOUT=* 
//*
//HFSPDSE DD DISP=SHR,DSN=HLQ.HFS 
//SAMP DD DISP=SHR,DSN=HLQ.SAMP 
//CONT DD DISP=SHR,DSN=HLQ.CONTENT 
//*
```

2. Edit the #LOADHFS member, and change the variable *HLQ* to the high-level qualifier according to your site standards.

3. Save the edited member as HFSLOAD.

   **Note**

   This step overwrites the customized data set that was created during installation.

4. Submit the HFSLOAD member JCL.

   **To enable or disable password caching**

   By default, when you create connections, the UIM server caches the password. However, you can enable and disable the password caching.

   1. Locate member #UPDADM in the UIM server sample library.
The following figure shows the default member #UPDADM.

**Figure 47: Default member #UPDADM**

```c
/*--------------------------------------------------------------
/*  Load the BMC HFS PDSE with SAMP library member to update the
/*  Password Caching setting.
/*--------------------------------------------------------------
*/

EXEC PGM=UIMHFSL,REGION=0K,
PARM='=b =version $UPDADM'
memname Samplib control cards member, default is $HFSLOAD.
t $UPDADM is an update of Password cache member only
   Activate tracing to SYSPRINT

STEPLIB DD DISP=SHR,DSN=HLQ.LOAD

SAS/C DD'S
SYSTERM DD SYSPRINT
SYSPRINT DD SYSPRINT
STGRPT DD SYSPRINT

STANDARD JOB DD'S
SYSUDUMP DD SYSPRINT

HFSPDSE DD DISP=SHR,DSN=HLQ,HFS
SAMP DD DISP=SHR,DSN=HLQ,SAMP
```

2 Edit member #UPDADM, and change *HLQ* to the high-level qualifier according to your site standards.

3 Save the edited member as UPDADMIN.

4 Save the edited member as UPDADMIN.

The following example shows the default member $ADMIN.

```
AllowPasswordCaching=true
```

5 Perform one of the following actions:

- To disable password caching, set `AllowPasswordCaching=false`.

- To enable password caching, set `AllowPasswordCaching=true`.

6 Save $ADMIN.

7 Submit the member UPDADMIN JCL.
Creating additional JCL Generation POFs

You can create additional JCL Generation POFs for each subsystem on each z/OS image by using the ISPF interface for the DASD MANAGER PLUS component.

Any JCL Generation POFs that you create in addition to the initial POF are considered user POFs (also called action POFs). For information about creating user or action POFs, see the *DASD MANAGER PLUS for DB2 User Guide*.

Merging multiple products into a single UIM server

Several BMC products for DB2 and IMS use the UIM server. You can merge multiple products into a single UIM server.

If you already have a UIM server installed on a z/OS image, and you install an additional product that uses the UIM server, you can merge the two UIM servers into a single UIM server and a single started task procedure.

For example, if you are installing the Database Performance for DB2 solution and you already have a UIM server installed for an IMS product (such as RECOVERY MANAGER for IMS), you can perform the steps in this section to enable the solution to work with your existing UIM server started task procedure.

**Note**
IMS products might require additional steps to merge into a single UIM server. For more information, see the documentation for your IMS product.

To merge multiple products into one UIM server

1. Locate the #UIMx member that the Installation System created in the UIM server sample library (*HLQ.XXSAMP*).
2. Copy the #UIMx member to your system procedure library and give the new member the name that you selected for the startup member during installation.
3. Ensure that the new UIM load library (*HLQ.XXLINK*) is first in the STEPLIB concatenation.
4. Add the older versions of the following files in concatenation order after the newer versions:
   - Application load library
The content files and the configuration files must be ordered from newest products and files to the oldest products and files.

The following figure shows an example of a consolidated started task procedure for the UIM server. This example UIM server works for Database Performance (DFD), an IMS product, and other DB2 products.

Figure 48: Consolidated #UIM member

```
//DFDUIMQ9 PROC M=DFDUIMQ9, <--- name of configuration member
//                             ENV=
//*--------------------------------------------------------------
//*                EXEC PGM=UIMMAIN,                              +
// REGION=0K, <--- specify region size +
// TIME=1440,ACCT=(5210),                                      +
// PARM=('-C &M &ENV -L =B =CNFTRACE =S =U =VERSION')          +
//* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
//*                            COMMON COMMAND-LINE PARAMETERS:    +
//* -C MMMMMM  CONFIGURATION FILE MEMBERNAME                   +
//* -P 9999 TCP LISTENER PORT NUMBER                          +
//* -L LOG MESSAGES AND TRACE VIA SUBTASK                    +
//* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
//* ENVIRONMENT VARIABLES TO CONTROL EXECUTION:              +
//* =SOUT= SPECIFY THE SYSOUT CLASS FOR DYNAMICALLY ALLOCATED +
// LOG FILES( IE. =SOUT=X )                                   +
// - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
//* SAS/C RUNTIME LIBRARY PARAMETERS:                        +
//* =B PRINT FUNCTION TRACEBACK WITH LIBRARY WARNINGS         +
//* =CNFTRACE PRINT DIAGNOSTICS DUE TO TCP/IP CONFIGURATION FAILURES +
//* =S PRINT STORAGE ANALYSIS REPORT AT TERMINATION           +
//* =U PRINT STORAGE USAGE REPORT AT TERMINATION              +
//* =VERSION PRINT RUNTIME LIBRARY RELEASE INFORMATION TO SYSTERM +
//* - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
// STEPLIB DD DISP=SHR,DSN=HLQ.XXLINK <--from new UIM/DHS installation
// DD DISP=SHR,DSN=DFD.LOAD <--from new DFD installation
// DD DISP=SHR,DSN=HLQ.IMLOAD <--from merged IMS installation
// DD DISP=SHR,DSN=HLQ.productCodeLOAD <--from nonmerged IMS installation
// DD DISP=SHR,DSN=DB2HLQ.DSNEXIT <--if other DB2 products installed
// DD DISP=SHR,DSN=DB2HLQ.DSNLOAD <--if DB2 products installed
//*--------------------------------------------------------------
```
5 Restart the UIM server address space.
Merging multiple products into a single UIM server
Verifying installation

After you customize and configure the products, you must verify the installation of the products.

Verifying the Administrative products’ installation

Use the following procedure to verify that ALTER, CATALOG MANAGER, CHANGE MANAGER, or DASD MANAGER PLUS have been installed correctly.

To verify the installation

1. Invoke the BMCDB2 CLIST.
2. On the COMMAND line, type CONTAB.
3. On the BMCDB2TB panel, verify that the correct partitioned data set (PDS) and member name are displayed in the library in which the BMCDB2 CLIST is located. The HLQ.CONTAB sequential file should also be displayed in the library.

   If the PDS and member name are not displayed, set the BMCDB2C variable in the BMCDB2 CLIST to the correct library.

4. Exit the CONTAB panel.
5. Select one of the products that you installed.
6. Access the environment information for the product that you have selected as follows:
   - In ALTER or CHANGE MANAGER, at the main menu, type ENVI on the Command line.
   - In CATALOG MANAGER, on the Primary Menu panel, type ENVI on the Command line.
In DASD MANAGER PLUS, at the main menu, select User Options. Then select Current environment information.

7 Review the environment panel to verify the displayed information.

**Note**

Generate an LO (Locations) list and verify the connections or attachments to other DB2 subsystems.

8 Exit the environment panel.

9 Repeat Step 5 on page 327 through Step 8 on page 328 for each product that you installed.

---

**Verifying Backup and Recovery product and Utility product installation**

The Installation System generates an installation verification procedure (IVP) job for each installed Backup and Recovery or Utility product. To help ensure that a product installed properly, BMC strongly recommends that you run the corresponding IVP job.

For products that use the dynamic bind process, the IVP job initializes that process by binding the necessary packages. Running the IVP job helps prevent subsequent bind problems, such as authorization problems, during product execution.

**Before you begin**

Complete the following tasks before running an IVP job:

- Submit all installation and customization jobs except the IVP job ($770IVP). For more information, see the Installation System documentation

- Apply the appropriate fixes for each product that you are installing. For instructions, see the Installation System documentation

- Grant the appropriate authorizations. For more information, see the customization information for the products that you have installed.
  If you are not the person who installed the products but are submitting the IVP job, ensure that you have the authorizations that are required to execute each product that was installed.

- Complete any additional customization tasks for your installed products or components.
To verify installation

1 If your jobs use data sets that are managed by the Storage Management Subsystem (SMS), ensure that the SMS service routine load library (SYS1.CSSLIB) is APF-authorized.

Complete this step regardless of whether SYS1.CSSLIB is in your system LNKLST or STEPLIB concatenation.

2 Use one of the following methods to edit either the EXEC statement in the product job step of the IVP job ($770IVP) or your job card:
   - Change the value of the REGION parameter to 0M.
   - If not already addressed by your site SMF defaults, add the MEMLIMIT parameter with an appropriate value for your site and the products that you are installing.

3 Submit the IVP job ($770IVP).

The IVP job should complete with condition code 0 unless otherwise indicated by comments in the job.

Note

The following temporary objects exist only for the duration of the IVP job:
   - Database BMCIVPDB
   - Table space BMCIVPDB.BMCIVPTS
   - Table BMC.BMCIVPTB
   - Table BMC.BMCIVPT2
   - Index BMC.BMCIVPIX1

Verifying the installation of System and SQL Performance products

The verification tasks you perform will depend on the products you are installing.

- If you installed SQL Explorer, APPTUNE, MainView for DB2 - Data Collector, or SQL Performance, you must start a product session and issue an Explain command.

MainView for DB2 - Data Collector users must access the menu from a MainView for DB2 Easy Menu.
For more information, see the MainView for DB2 User Guide.
- If you installed SQL Performance, you must verify that you can access the Index Component reports.

- If you installed SQL Explorer or SQL Performance, you must also verify the SQL Explorer installation.

- If you installed Pool Advisor or System Performance, you must start a product session and start a reporting session.

The following steps summarize the System and SQL Performance products verification tasks and the products for which you must run them.

<table>
<thead>
<tr>
<th>Step</th>
<th>Procedures</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>“Starting the DBC subsystem” on page 330</td>
<td>All products except SQL Explorer and OPERTUNE</td>
</tr>
<tr>
<td>2</td>
<td>“Checking the system console log messages” on page 331</td>
<td>All products except SQL Explorer and OPERTUNE</td>
</tr>
<tr>
<td>3</td>
<td>“Starting a product session” on page 335</td>
<td>All products</td>
</tr>
<tr>
<td>4</td>
<td>“Selecting a DOMPLEX” on page 335</td>
<td>All products except SQL Explorer and OPERTUNE</td>
</tr>
<tr>
<td>5</td>
<td>“Issuing a dynamic Explain command” on page 336</td>
<td>SQL Explorer APPTUNE MainView for DB2 - Data Collector SQL Performance</td>
</tr>
<tr>
<td>6</td>
<td>“Accessing the Index Component reports” on page 340</td>
<td>SQL Performance</td>
</tr>
<tr>
<td>7</td>
<td>“Verifying the SQL Explorer installation” on page 342</td>
<td>SQL Explorer SQL Performance</td>
</tr>
<tr>
<td>8</td>
<td>“Starting a Pool Advisor or System Performance reporting session” on page 349</td>
<td>Pool Advisor System Performance</td>
</tr>
</tbody>
</table>

**Starting the DBC subsystem**

This task is *required* for all products except for SQL Explorer or OPERTUNE. The product procedure (PROC) must be invoked to initialize the DBC. One DBC subsystem can monitor multiple DB2 subsystems on one z/OS. The DB2 subsystems to be monitored were specified in the DOMPLEX option set. The DBC can be invoked as a z/OS started task or as a batch job.
Invoking the DBC subsystem as a started task

The DBC subsystem is started during installation. If you need to restart it, use this procedure.

Issue the MVS START command for the started task created from DBC$STC (see “Editing or reviewing the DBC JCL procedure” on page 237):

/S DBC$STC

--- Note ---
You can also issue the MVS START command for the started task by specifying START dbc_ProcName. Normally, the DBC will start all of the installed agents, including the Data Collector agent.

**Warning!** Do not use the name of the DB2 subsystem.

--- WARNING ---
Do not use the name of the DB2 subsystem.

Invoking the DBC subsystem as a batch Job

Submit the JCL created when you edited the JCL procedures (see “Editing or reviewing the DBC JCL procedure” on page 237).

To stop the batch job, issue the following command:

/p jobName

When you stop the batch job, you must also stop the initiator under which the batch job ran by issuing the /p (purge) command.

--- Note ---
The DBC subsystem is a long-running-service address space that normally remains active for the life of an IPL. Therefore, BMC does not recommend starting the DBC subsystem as a batch job. Doing so causes the JES initiator to be busy for the life of the DBC subsystem. If you want to run the DBC as a batch job, replace the PROC statement with a valid JCL job card.

Checking the system console log messages

Watch the system console log for the messages issued by the product procedure (PROC).
When the DBC and Data Collector become active, messages similar to those shown in the JES Job Log and SYSPRINT Messages Report (Figure 49 on page 332) are displayed.

**Note**

DSNW133I messages (Trace data set lost. Destination not accessible.) are sometimes issued by DB2 while the Data Collector is starting. You can ignore these messages. The messages will stop after the Data Collector starts and makes contact with DB2.

**Pool Advisor and BMC System Performance only:** The Data Collector performs an object scan every night and issues messages BMC23510 and BMC23511 for each DB2 it monitors, marking the beginning and end of the scan.

**To check the system console log messages**

1. Verify the licensing for your installed products.

   Lines that begin with BMC24907 contain the licensing information for your installed products.

2. Verify the subsystem and plan names.

   Lines that begin with BMC24951 contain information about the subsystems and plans that are recognized by the Data Collector, as shown in the following example:

   ```
   BMC24951 DOM7 DB2=DEC7 Rel=810 Char=*DEC7 Status=UP Plan=DAAvyrD1
   ```

   **Note**

   This information is stored in the DOMPLEX option set. The Data Collector uses these plans to perform Explain operations. If you bind one of these plans under a different name, the Explain process will fail.

3. On the Command line in the system console, type `/dbcssid APPSTAT`, where `dbcssid` is the subsystem ID of the local DBC previously specified in the DOMPLEX option set.

   The statuses of all DB2s that are recognized by the Data Collector are displayed.

---

**Figure 49: JES job log and SYSPRINT messages report**

```plaintext
JES2 JOB LOG -- SYSTEM DB2B -- NODE BMCPXL1
23.28.50 STC27629 ---- FRIDAY, 25 APR 2015 ----
23.28.50 STC27629 IEF695I START DBCRI101 WITH JOBNAME DBCRI101 IS ASSIGNED TO USER BMCDB2, GROUP SYS1
23.28.50 STC27629 $HASP373 DBCRI101 STARTED
23.28.50 STC27629 IEF403I DBCRI101 - STARTED - TIME=23.28.50
23.28.52 STC27629 BMCDBC0088I 23.28.52 DC2B DBC version 10.1.00 initialization complete
23.28.55 STC27629 BMC24907 DC2B POOL ADVISOR LICENSE VERIFIED FOR THIS PROCESSOR
23.28.55 STC27629 BMC24907 DC2B SYSP PERFORMANCE LICENSE VERIFIED FOR THIS PROCESSOR
23.28.55 STC27629 BMC24907 DC2B SQL EXPLORER LICENSE VERIFIED FOR THIS PROCESSOR
23.28.55 STC27629 BMC24907 DC2B SQL PERFORMANCE LICENSE VERIFIED FOR THIS PROCESSOR
```
Verifying the installation of System and SQL Performance products

BMC Products and Solutions for DB2 Customization Guide

334
Detailed information for all messages is available in the online Help. Type `HELP <messageID>` on the **Command** line of any System and SQL Performance product panel and press **Enter**.

To stop this DBC subsystem at a later time, use the MVS STOP command as follows:

```
P dbcssid
```

where `dbcssid` is the name of your DBC.

If the DBC is being run as a batch job, use the following MVS STOP command:

```
P jobName
```

where `jobName` is the DBC batch job.

When the STOP command is issued, a list of messages is displayed. Detailed information for all messages is available in online Help.

---

**Note**

You can issue MVS START and STOP commands from the operator console or SDSF.

---

### Starting a product session

If you previously terminated your session, see “Starting a product session” on page 248 for instructions to invoke the product. Otherwise, the product’s main menu is still displayed.

### Selecting a DOMPLEX

The product selects a DOMPLEX automatically if there is a DOMPLEX with a compatible Data Collector active when you begin your session.
If no Data Collector is selected (the Current Data Collector field is blank), follow these directions to select a Data Collector:

**To select a DOMPLEX**

1. Display the DOMPLEX Selection panel (Figure 50 on page 336).

   The DOMPLEXes option appears on all main menus, but the option number is not the same on all main menus. Select the option that is labeled DOMPLEXes.

   **Figure 50: DOMPLEX Selection panel**

   ![DOMPLEX Selection panel](image)

   Current Data Collector : Status :
   Select a DOMPLEX from the following list to be the data source for future requests. Press Enter to process the new selection.

<table>
<thead>
<tr>
<th>Sel</th>
<th>DOMPLEX</th>
<th>DC SSID</th>
<th>Description</th>
<th>Status</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DC01</td>
<td>DC01</td>
<td>DEFAULT PROFILE</td>
<td>ACTIVE</td>
<td>COMPATIBLE</td>
</tr>
<tr>
<td></td>
<td>LOCAL DB2S: DB2S DB21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Select a DOMPLEX from the list of defined DOMPLEXes.

   Select a DOMPLEX with a compatible Data Collector that has a Status of ACTIVE.

   **Note**

   If no DOMPLEX with an active compatible Data Collector is available, return to “Verifying the installation of System and SQL Performance products” on page 329 and start a Data Collector.

   Type S in the Sel field beside the DOMPLEX name and press Enter.

3. Press F3 (End) to return to the main menu.

**Issuing a dynamic Explain command**

This task applies only to APPTUNE, MainView for DB2 - Data Collector, and SQL Performance.

The successful execution of an Explain command confirms that the Report Manager is communicating with the Data Collector, that the Data Collector is communicating with DB2, that the DAA vrD1 plan is working, and that installation is complete.
To issue a dynamic Explain command

1 Display the Explain Object Specification panel (Figure 51 on page 337).

- From the APPTUNE Main Menu, select option 3 (Explain Interface) and press Enter.

- From the System and SQL Performance main menu, select option Q (APPTUNE and Index Component), then select option 3 (Explain Interface), and press Enter.

- From MainView for DB2, hyperlink from the THDDETL view for a long-running thread to access a report from which you can invoke the dynamic Explain for the active SQL statement. For more information, see the MainView for DB2 User Guide.

2 Complete the Explain Object Specification panel as follows:

   a Specify a DB2 subsystem in the SSID field.

   b Type 5 in the Type field.

   c Press Enter.

An edit session is displayed (Figure 52 on page 337).

Figure 52: Ad hoc SQL Explain edit session

---

Chapter 12 Verifying installation 337
3 In the edit window, type `SELECT * FROM SYSTABLES WHERE NAME = :H` and press F3.

The Explain or Execute Parameters panel (Figure 53 on page 338) is displayed.

**Figure 53: Explain or Execute Parameters panel (PSSPA117)**

```
PSSPA117 ----------------- Explain or Execute Parameters ----------------------
Command ===> Specify the options below and press ENTER to continue.
Option ............ 1    1. Explain   
    2. Execute   
    3. Edit     
Qualifier Name . . . . SYSIBM
```

4 Complete the Explain or Execute Parameters panel as follows:

a Type 1 in the **Option** field.

b Type **SYSIBM** in the **Qualifier Name** field.

c Press **Enter** to display the Explain Results panel (Figure 54 on page 338).

**Note**

Actions shown in bold in Figure 54 on page 338 are available only if you have applied the SQL Performance solution password. They will not be displayed for an SQL Explorer-only installation.

**Figure 54: Explain Results panel (PSSPE200)**

```
FILE COMMANDS OPTIONS HELP
----------------------------------------------
PSSPW200                        Explain Results for 
SOLTEXT                         SQLTEXT
Command ===> SCROLL ===>> CSR
More: >
Actions: S H R RS RW RI XD XS W P T C D U IM SA
LBL  STMTNO COST RATE SQL-STATEMENT
XDO1  114690.937500 select * from systables ; 
COST RATE QB PL MIX QTYPE METH ACC MATCH IX TBNAME IXNAME
XDO1  114690.93 1 1 0 SELECT 0 R 0 N SYSTABLES
```

5 Verify that the Explain executed correctly by reviewing the Explain Results.

The Explain Results panel displays COST information associated with the Explain.
Tip
You can type action codes next to the statement area or access path area on the Explain Report to see more information. To view all information on the Explain Results panel, press F11 to scroll to the right and press F10 to scroll to the left.

a If the command returns a negative SQL code instead of Explain text, verify the following conditions:

- The plan table that was used is the correct format for the version of DB2.

Note
To check which plan table was used, perform the following steps:

1 Press F3 from the SQL Error panel.

2 On the Explain Results for SQLTEXT panel (PSSPW200), put your cursor on OPTIONS in the task bar and hit Enter.

3 Choose option 1 (Explain).

4 Check the plan tables in the DB2 subsystem that have the creator of the value listed in the Plan Table Owner field.

b If you receive an SQLCODE=100 warning, check to make sure that the $781PERF job was run.

This job creates a stand-alone database and tablespace that the product uses to create user plan tables, if needed. A dummy PLANTBL table is also created with the alias BMCPSS_PLANTBL. The product uses this alias to find the database and tablespace if plan tables need to be created. If the product cannot find this alias, you will receive an SQLCODE=100, NOT FOUND warning.

The database, tablespace, and PLANTBL table may persist from release to release. Make sure that the alias qualifier matches the qualifier used in the BIND of the PSS packages.
Note

If your DB2 subsystem was recently migrated to DB2 Version 10 or later, the Explain request will fail unless all of the Explain tables being used are in a UNICODE tablespace and are in the DB2 Version 10 Explain schema. IBM provides the following jobs to identify and convert user plan tables: DSNTIJPM, DSNTIJXA, DSNTIJXB, and DSNTIJCX. If the plan tables do not exist, they will be created in the tablespace for the System and SQL Performance for DB2 products. BMCUPLAN is the default tablespace name.

If one or more of these conditions were not met, correct them and repeat the steps in this procedure. If you cannot determine why the command failed, contact BMC Customer Support for assistance.

Where to go from here

When you have successfully produced the Explain Results, the verification procedure for APPTUNE and MainView for DB2 - Data Collector is complete.

If you are also installing SQL Explorer or SQL Performance, you must verify the SQL Explorer installation.

Accessing the Index Component reports

This task applies only to SQL Performance. The display of the Index Component reports confirms that the Index Component of SQL Performance has been installed correctly.

To access the Index Component reports

1. From the System and SQL Performance for DB2 main menu (Figure 27 on page 228, select option Q (APPTUNE and Index Component) and press Enter.

The APPTUNE and Index Component Main Menu (Figure 55 on page 340) is displayed.

Figure 55: APPTUNE and Index Component Main Menu (DOMEPLN3)
2 Select option 1 (SQL Workload) and press Enter.

The SQL Workload Analysis Menu (Figure 56 on page 341) is displayed.

Figure 56: SQL Workload Analysis Menu (ASQEWAM1)

3 Select option 2 (Workload analysis) and press Enter.

The SQL Workload Initial Analysis Level panel (Figure 58 on page 342 is displayed.

Figure 57: SQL Workload Initial Analysis Level panel (DOMEPNL3)

4 Select option 21 (Subsystem Getpage Volume) and press Enter.
The SQL Workload Analysis Menu (Figure 58 on page 342) is displayed.

**Figure 58: SQL Workload Analysis Menu (ASQEWAM1)**

ASQEWAM1/I               SQL Workload Analysis Menu                   13:40:14
Command ===> ________________________________________________________________

Report Criteria:
Source of data . . . : Subsystem DOMS
For DB2 SSIDs . . . . : *
Duration . . . . . . : No time limit
Initial report . . . : INDEX SUBSYSTEM GETPAGE VOLUME
Application profile . : DEFAULT           Owner :

Select one of the following options to change the report criteria or
to begin reporting.

1. Workload analysis - Begin workload reporting
2. Initial report - Select the initial report to be viewed
3. Report type - Select the report type (data or graph)
4. Application profile - Select the profile for group reporting
5. Time interval - Specify the time frame for reporting
6. Data source, DB2(s) - Select data source and DB2 subsystems

Select option 1 (Workload analysis) and press Enter.

The Subsystem Getpage Volume report (Figure 59 on page 342) is displayed.

**Figure 59: Subsystem Getpage Volume report**

ASQEQRPW/I                      View a Report                      LINE 1 OF 1
Command ===> _______________________________________________ Scroll ===> CSR_
BMCStwrd.IOODSTAT    --    SUBSYSTEM GETPAGE VOLUME    --       09/29 14:18:31
-----------------------------------------------------------------------------------------------------------------------
Actions: B-Table/Index Breakdown  A-Table Getpage
Logical DB2 Name  Index%  Stmt /Stnt    AvgTime   Number AvgTime   Number    Pages     Stmts     Stmts  Stmt %
---------  ------  ------ -------- -------  ------- -------  --------  --------  --------  --------  ------
+ DECA 8.0%   36.0  10488252 0.00001     2617 0.00472       460      8861    291152    162789    55.9  DECA

If the report is not displayed, ensure that the Data Collector is monitoring the DB2 subsystems and that you are collecting object information.

6 If the report is not displayed, ensure that the Data Collector is monitoring the DB2 subsystems and that you are collecting object information.

**Verifying the SQL Explorer installation**

To verify that SQL Explorer has been installed correctly, you must test the following functions:

- Call Attach facility (CAF)
- Impact Analysis
- Distributed Data facility (DDF)
Note
Each of these tests begins at the SQL Explorer main menu. Select option 0 from the main menu to change any default values before you begin.

Testing the Call Attach Facility

Use the following procedure to test the Call Attach Facility:

1. From the System and SQL Performance main menu, select option S (SQL Explorer Component) and press Enter.

   The SQL Explorer Menu is displayed.

2. Select option 1 (Explain), type the subsystem ID of an active, local DB2 subsystem in the SSID field, and press Enter.

   The Explain Object Specification panel is displayed.

3. Complete the Explain Object Specification panel as follows:
   - Type 2 in the Type field.
   - Type % in the Package: COLLID field (% is a wildcard).
   - Type PSSXSQL in the Package: Name field.
   - Type % in the Package: Version field.
   - Type L (List Objects) in the Processing Mode field.

4. Press Enter to display the Explain Object Selection List panel.

   At least one entry for package PSSXSQL should be displayed on the Explain Object Selection List panel. This entry verifies that CAF is working. Multiple entries indicate that more than one version of SQL Explorer is installed.

5. Type S next to one of the PSSXSQL packages, and press Enter to display a list of statements.

6. Type XD next to one of the statements, and press Enter to execute a dynamic Explain.

   The Explain Results panel is displayed.

7. Verify that the Explain executed correctly by reviewing the Explain results.

   The Explain Results panel displays COST information associated with the Explain.
You can type action codes next to the statement area or access path area on the Explain Results panel to see more information. To view all information on the Explain Results panel, press **F11** to scroll to the right and press **F10** to scroll to the left.

**a** If the command returns a negative SQL code instead of Explain text, verify the following conditions:

- The plan table that was used is the correct format for the version of DB2.

**Note**

To check which plan table was used, perform the following steps:

1. Press **F3** from the SQL Error panel.
2. On the Explain Results for SQLTEXT panel (PSSPW200), put your cursor on OPTIONS in the task bar and hit **Enter**.
3. Choose option 1 (Explain).
4. Check the plan tables in the DB2 subsystem that have the creator of the value listed in the **Plan Table Owner** field.

- The plan name was specified correctly in the PSS2 ssid member in the UBBSAMP or your runtime SAMP data set that is allocated to the PSSCNTL DD.

**b** If you receive an SQLCODE=100 warning, check to make sure that the $781PERF job was run.

This job creates a stand-alone database and tablespace that the product uses to create user plan tables, if needed. A dummy PLANTBL table is also created with the alias BMCPSS_PLANTBL. The product uses this alias to find the database and tablespace if plan tables need to be created. If the product cannot find this alias, you will receive an SQLCODE=100, NOT FOUND warning.

The database, tablespace, and PLANTBL table can persist from release to release. Make sure that the alias qualifier matches the qualifier used in the BIND of the PSS packages.
If your DB2 subsystem was recently migrated to DB2 Version 10 or later, the Explain request will fail unless all of the Explain tables being used are in a UNICODE tablespace and are in the DB2 Version 10 Explain schema. IBM provides the following jobs to identify and convert user plan tables: DSNTIJPM, DSNTIJXA, DSNTIJXB, and DSNTIJCX. If the plan tables do not exist, they will be created in the tablespace for the System and SQL Performance for DB2 products. BMCUPLAN is the default tablespace name.

8 If one or more of these conditions were not met, correct them and repeat Step 6 on page 343. If you cannot determine why the command failed, contact BMC Software Customer Support for assistance.

Testing Impact Analysis

To test Impact Analysis, complete the following steps:

1 Return to the SQL Explorer menu (PSSPF000).

2 Select option 5 (Impact Analysis).

3 Type the subsystem ID of an active, local DB2 in the SSID field, and press Enter.

The Impact Analysis Object Specification panel (Figure 60 on page 345) is displayed.

**Figure 60: Impact Analysis Object Specification panel (PSSPI010)**

PSSPI010----------------- Impact Analysis Object Specification --------------------
Command ===>

Process Mode  O (O=Online, B=Batch)

Objects to Analyze (Case-Sensitive): (Table, View, Alias)
  Creator . . % Name . . . BMCPSS_BASE

Columns: (Comma-Delimited List)
  Name . . APPLNAME

For the specified table objects, search only these DBRMs and packages:
Type . . . . 2 (1=DBRM, 2=Package, 3=DRBM and Packages)

DBRM:
  Plan . . Name . . %

Package:
  COLLID . . % Name . . PSSXSQL
  Version %

Options

4 Complete the Impact Analysis Object Specifications panel as follows:

- Type O in the Process Mode field.
- Type % in the Creator field.
- Type BMCPSS_BASE in capital letters in the Name field.
- Type APPLNAME in capital letters in the Columns: Name field.
- Type 2 in the Type field.
- Type % in the Package: COLLID field (% is a wildcard).
- Type PSSXSQL in the Package: Name field.
- Type % in the Package: Version field.

5 Press Enter to execute online Impact Analysis.

**Note**

If any of the data sets do not exist, the Allocate Data Set panel is displayed. Allocate the product data sets if prompted.


The Summary report should list one impacted SELECT statement in each PSSXSQL package that is listed. The Summary will also show a mixed list of the impacted base table.

7 If the command returns a negative SQL code instead of the Impact Analysis Summary report, verify that the plan name was specified correctly in the PSS2ssid member in the LLQSAMP (where LLQ is DB, XX, BB, and UBB) data that is allocated to the PSSCNTL DD.

8 If one or more of these conditions were not met, correct them and repeat the procedure. If you cannot determine why the command failed, contact BMC Software Customer Support for assistance.

If you are not using the Distributed Data Facility (DDF), you have finished the verification process for SQL Explorer and SQL Performance. If you are using the DDF, continue to the next task

### Testing the Distributed Data Facility

Use the following procedure to test the Distributed Data Facility.

1 Return to the SQL Explorer menu (PSSPF000).
2 Select option 1, type the subsystem ID of an active, local DB2 in the SSID field, type the location of a remote DB2 in the DDF Location field, and press Enter.

The Explain ObjectSpecification panel is displayed.

3 If the values previously typed in the fields on the Explain Object Specification panel are no longer displayed, use the values from Figure 51 on page 337. Press Enter to display the Explain Object Selection List panel.

At least one entry for package PSSXSQL should be displayed on the Explain Object Specification List panel if SQL Explorer is installed at the remote site and its location name is in the communications database for the subsystem to which you are connecting. Multiple entries indicate that more than one version of SQL Explorer is installed.

4 Type S next to one of the PSSXSQL packages and press Enter to display a list of statements.

5 Type XD next to one of the statements and press Enter to execute a dynamic Explain.

The Explain Results panel is displayed.

6 Verify that the Explain executed correctly by reviewing the Explain results.

The Explain Results panel displays COST information associated with the Explain.

You can type action codes next to the statement area or access path area on the Explain Results panel to see more information. To view all information on the Explain Results panel, press F11 to scroll to the right and press F10 to scroll to the left.

If the command returns a negative SQL code instead of Explain text, verify the following conditions:

- The plan table that was used is the correct format for the version of DB2.
Note
To check which plan table was used, perform the following steps:

1. Press F3 from the SQL Error panel.

2. On the Explain Results for SQLTEXT panel (PSSPW200), put your cursor on OPTIONS in the task bar and hit Enter.

3. Choose option 1 (Explain).

4. Check the plan tables in the DB2 subsystem that have the creator of the value listed in the Plan Table Owner field.

- The plan name was specified correctly in the PSS2 ssid member in the LLQ SAMP (where LLQ is DB, XX, BB, and UBB) data set that is allocated to the PSSCNTL DD.

7. If you receive an SQLCODE=100 warning, check to make sure that the $781PERF job was run.

   This job creates a stand-alone database and tablespace that the product uses to create user plan tables, if needed. A dummy PLANTBL table is also created with the alias BMCPSS_PLANTBL. The product uses this alias to find the database and tablespace if plan tables need to be created. If the product cannot find this alias, you will receive an SQLCODE=100, NOT FOUND warning.

   The database, tablespace, and PLANTBL table may persist from release to release. Make sure that the alias qualifier matches the qualifier used in the BIND of the PSS packages.

Note
If your DB2 subsystem was recently migrated to DB2 Version 10 or later, the Explain request will fail unless all of the Explain tables being used are in a UNICODE tablespace and are in the DB2 Version 10 Explain schema. IBM provides the following jobs to identify and convert user plan tables: DSNTIJPM, DSNTIJXA, DSNTIJXB, and DSNTIJCX. If the plan tables do not exist, they will be created in the tablespace for the System and SQL Performance for DB2 products. BMCUPLAN is the default tablespace name.

8. If one or more of these conditions were not met, correct them and repeat Step 5 on page 347. If you cannot determine why the command failed, contact BMC Software Customer Support for assistance.

When you have successfully completed these steps, you have finished the verification process for SQL Explorer and SQL Performance.
Starting a Pool Advisor or System Performance reporting session

Use the following procedure to start a Pool Advisor or BMC System Performance reporting session.

1. Select option **P (Pool Advisor)** from the Pool Advisor main menu, or select option **D (BMC System Performance)** from the BMC System Performance main menu.

   The DB2 Pools Status Monitor report (PMDMAIN) is displayed for Pool Advisor.

   ![PMDMAIN Report Example](image)

   The Sysplex DB2 Monitor report (SPDMAIN) is displayed for BMC System Performance.

   ![SPDMAIN Report Example](image)

2. Verify that data is present from the DB2 subsystems defined to the selected Data Collector.

When you have successfully activated the DB2 Pools Status Monitor report or the Sysplex DB2 Monitor report showing current data, you have finished the verification process for Pool Advisor and BMC System Performance.

Verifying the installation of NGT products

Use the following procedure to verify that the installation of NGT products was properly completed.
This example tests the installation of the NGT Reorg product. If you have the appropriate license, you can run the test on any NGT product by editing the SYSIN statement accordingly.

1. Copy the member from the NGTCNTL (or BMCCNTL) data set to UNGTCNTL (or UBMCCNTL), and then open MASTERJB for editing.

2. Replace all references of YOURDB2 with your DB2 high level qualifier.

   **Example**
   
   If your high-level qualifier is DSN1210.DSN1, you should replace all references of YOURDB2 with DSN1210.

3. Replace all references of YOURNGT with your NGT high level qualifier.

   **Example**
   
   If your high-level qualifier is SYS2.NGT you should replace all references of YOURNGT with SYS2.NGT.

4. In the //NGTUSTEP EXEC statement `PARM=SSID`, replace SSID with the subsystem identifier of your DB2 subsystem.

5. Update the SYSIN statements with a database and table space name.

   You may also substitute the control statement of NGT Reorg with a control statement for another licensed NGT product.

6. Add a job card to the top of the file.

7. Submit the job.

   A successful completion code indicates that the BMC Next Generation Technology (NGT) utility products are ready for use.

**Note**

Some BMC Next Generation Technology (NGT) utility products might require additional data sets when they are executed. For more information, see the relevant NGT product reference manual.

**Editing allocation automation**

Use the following procedures to setup the allocation automation. You must complete all these procedures.
To allocate work files

1. Copy the NGTAUTO data set to UNGAUTO.

2. In UNGAUTO, open XSUTDBMG for editing.

   This automation control point file controls the creation and extension of the NGT Work File VSAM data sets for job executions.

3. Locate all comments in the JCL that indicate which lines can be updated with the correct volume or SMS. If you are using SMS you will probably not need to change anything.

4. Save the file.

   The file is executed each time you run a NGT utility product job.

To allocate copy data sets

1. Copy the NGTAUTO data set to UNGAUTO.

2. In UNGAUTO, open member XCPYDYNM for editing.

3. In the DATASET subroutine, set the GDGLIMIT, and edit the DSNAME to the naming standard that you use for image copy data set names.

   If you are migrating from a previous version of BMC Next Generation Technology (NGT) utility products, you can cut and paste your prior logic here.

4. Save the file.

   The file is executed each time you run a NGT utility product job that creates an image copy.

To create a server job card model JCL

1. Copy the NGTAUTO data set to UNGAUTO.

2. In UNGAUTO, open member SVRJOBCD for editing.

3. In the DBEXEC data set, open member SVRJOBCD for editing.

4. You may edit the job name mask in the first line of this file, but it is only necessary if you have shop standards that enforce job names.

   The job name mask controls the naming of server jobs automatically generated during NGT product processing. For more information on creating job name
masks, see the section about literals for job and step name in the *BMC Next Generation Technology General User Guide*.

5 Save the file.

This job card model is used each time you run a NGT utility product job.
Migrating to a different version of DB2

This topic describes how to migrate or fall back to a different version of DB2.

*Migration* is the process of upgrading from one version or mode of DB2 to a later version or mode.

*Fallback* is the process of returning to an earlier version of DB2. This topic provides the procedures that you must perform to ensure that the BMC products continue to execute after migration or fallback.

Supported DB2 versions and modes

Ensure that your product versions support the DB2 version to which you are migrating or falling back, as listed in the following table.

**Note**

For information about support for DB2 versions, review your BMC product release notes.

<table>
<thead>
<tr>
<th>BMC product</th>
<th>DB2 Version 9 or 10</th>
<th>DB2 Version 11</th>
<th>DB2 Version 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALTER or CHANGE MANAGER</td>
<td>10.1.00</td>
<td>11.1.00, 11.2.00</td>
<td>12.1.00</td>
</tr>
<tr>
<td>APPTUNE</td>
<td>10.1.00</td>
<td>11.1.00, 11.2.00</td>
<td>12.1.00</td>
</tr>
<tr>
<td>CATALOG MANAGER</td>
<td>10.1.00</td>
<td>11.1.00, 11.2.00</td>
<td>12.1.00</td>
</tr>
<tr>
<td>CHECK PLUS</td>
<td>10.1.00</td>
<td>11.1.00, 11.2.00</td>
<td>(toleration only) 11.2.00 with PTFs BPU8707 and BPU8789</td>
</tr>
<tr>
<td>COPY PLUS</td>
<td>10.1.00</td>
<td>11.1.00, 11.2.00</td>
<td>NONE</td>
</tr>
</tbody>
</table>
The BMC products for DB2 support the following DB2 Versions:

- DB2 V12 Function level 100
- DB2 V12 Function level 500
- DB2 V11 Conversion mode (CM)
New DB2 version migration

This topic describes the process of upgrading from one version or mode of DB2 to a later version or mode.

Administrative products and solutions

When you migrate to a new version or mode of DB2, you must perform certain tasks to ensure that the Administrative products continue to execute.

**Note**
In procedures, ssid refers to the DB2 subsystem ID, and HLQ refers to the high-level qualifier that your site uses.

Migrating to DB2 Version 12 function level 500 from Version 11

Complete the appropriate procedures to migrate your Administrative products from DB2 Version 11 new-function mode to DB2 Version 12.

To migrate ALTER or CHANGE MANAGER version 12.1 or later

1. Migrate the DB2 catalog.

2. Run all of the following bind jobs from HLQUBMCCNTL:
   - ACMssidP
   - ACSssidP
   - AEXssidP

3. Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.
To migrate CATALOG MANAGER version 12.1 or later

1 Migrate the DB2 catalog.

2 Run the following bind jobs from HLQ.UBMCCNTL:
   - ACTssidP
   - DAAssidP or PS1ssidP
   - AEXssidP

3 Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.

To migrate DASD MANAGER PLUS version 12.1 or later

1 Migrate the DB2 catalog.

2 Run the following bind jobs from HLQ.UBMCCNTL:
   - ASUssidP
   - ACSssidP
   - ATSssidP
   - AEXssidP

3 Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.

To migrate BMC Workbench version or 12.1

1 Issue the following console command to stop the GUD agents:
   `/dbcssid GUD,STOPALL.

   **Note**
   The `dbcssid` value represents the DBC subsystem ID.

2 Migrate your DB2 catalog.

3 Issue the following console command to start your GUD agents:
   `/dbcssid GUD,STARTALL

Migrating to DB2 Version 11 new-function mode from Version 10

Complete the appropriate procedures to migrate your Administrative products from DB2 Version 10 new-function mode to DB2 Version 11.
You can migrate to any of the following DB2 Version 11 modes:

- Conversion mode
- Enabling-new-function mode
- New-function mode (NFM)

**To migrate ALTER or CHANGE MANAGER version 11.1 or 11.2**

1. Migrate the DB2 catalog.

2. Run all of the following bind jobs from `HLQ.UBMCCNTL`:
   - `ACMssidP`
   - `ACSssidP`
   - `AEXssidP`

3. Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.

**To migrate CATALOG MANAGER version 11.1 or 11.2**

1. Migrate the DB2 catalog.

2. Run the following bind jobs from `HLQ.UBMCCNTL`:
   - `ACTssidP`
   - `DAAssidP` or `PS1ssidP`
   - `AEXssidP`

3. Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.

**To migrate DASD MANAGER PLUS version 11.1 or 11.2**

1. Migrate the DB2 catalog.

2. Run the following bind jobs from `HLQ.UBMCCNTL`:
   - `ASUssidP`
   - `ACSssidP`
   - `ATSssidP`
   - `AEXssidP`

3. Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.
To migrate BMC Workbench version 1.0 or 1.1

1 Issue the following console command to stop the GUD agents:
   `/dbcssid GUD,STOPALL`.

   **Note**
   The `dbcssid` value represents the DBC subsystem ID.

2 Migrate your DB2 catalog.

3 Issue the following console command to start your GUD agents:
   `/dbcssid GUD,STARTALL`

**Migrating to DB2 Version 10 from Version 9 new-function mode**

Complete the appropriate procedures to migrate your Administrative products from DB2 Version 9 new-function mode to DB2 Version 10.

You can migrate to DB2 Version 10 New-function mode (NFM).

**To migrate ALTER or CHANGE MANAGER version 10.1 or later**

1 Migrate the DB2 catalog.

2 Run all of the following bind jobs from `HLQ.UBMCCNTL`:
   - ACMssidP
   - ACSssidP
   - AEXssidP

3 Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.

**To migrate CATALOG MANAGER version 10.1 or later**

1 Migrate the DB2 catalog.

2 Run all the following bind jobs from `HLQ.UBMCCNTL`:
   - ACTssidP
   - AEXssidP

3 *(CATALOG MANAGER version 11.1.00 and later)* Run the `HLQ.UBMCCNTL(PS1ssidP)` or `HLQ.UBMCCNTL(DAAssidP)` bind job.
4 Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.

To migrate DASD MANAGER PLUS version 10.1 or later

1 Migrate the DB2 catalog.

2 Run the following bind jobs from HLQ.UBMCCNTL:
   - ASussidP
   - ACSssidP
   - ATSssidP
   - AEYssidP

3 Complete the migration procedure, see “Completing the migration to a new version of DB2” on page 360.

To migrate BMC Workbench for DB2 version 1.0 or later

1 Issue the following console command to stop the BMC Workbench agents:
   /dbcssid GUD,STOPALL.

   Note
   The dbcssid value represents the DBC subsystem ID.

2 Migrate your DB2 catalog to DB2 Version 10.

3 If SYSIBM.SYSPACKSTMT has not been converted to the new format and Automatic Rebind (ABIND) is set to NO on your subsystem, run these jobs:
   - Run DAAssidP or PS1ssidP (bind packages) to rebind all packages.
   - Run DAAssidB or PS1ssidB (bind plan) to bind the plan.

   Note
   The ssid value represents the DB2 subsystem ID.
   Either DAA* bind jobs or PS1* bind jobs are available, depending on which solution is installed. The bind jobs are in the UBMCCNTL or UBMCSAMP data set.

4 Convert the user plan tables to unicode by using the following sample jobs from IBM:
   - DSNTIJPM
   - DSNTIHXA
   - DSNTIJXB
DSNTIJXC

You are now operating the BMC product environment in exploitation mode.

5 Issue the following console command to start your GUD agents:
   `/dbcssid GUD,STARTALL`

**Completing the migration to a new version of DB2**

Perform the following procedure to verify the values for the DB2EXIT and DB2LOAD libraries.

1 Verify the values for the libraries in the product options file (POF).
   a Edit the POF in your `HLQ.UBMCCNTL` data set. The name of the file is specified in the `POFDS` keyword in the installation options module for your product.
   b Ensure that the values for the DB2EXIT and DB2LOAD keywords are correct for the version of DB2 to which you have migrated.

2 If you modified the values in the POF in step 1, refresh the POF. When you refresh the POF, users receive the updated values.
   a Edit the initial POF outside of the product.
   b Change the value of the `POFDATE` keyword to the current date.
   c Append the refresh attribute `(R)` to the values that you want to update.
   d Save the POF.
   e *(for runtime data sets)* Copy the POF from `HLQ.UBMCCNTL` to `HLQ.BMCCNTL`.

3 Verify the values for the libraries in the control table.
   a Edit the control table in the `HLQ.CONTAB` data set.
   b Ensure that the location and name of the DB2EXIT and DB2LOAD libraries are correct for the version of DB2 to which you have migrated. For example:

```
*LIB SSID Data Set Name
*-----|---------------|-------------------------------|
EXIT DB11 'SYS3.DB11.DSNEXIT'     *
LOAD DB11 'SYS2.DB2V11M.DSNLOAD'   *
```
Backup and Recovery and Utility products and solutions

For the Backup and Recovery and Utility products, run the $770IVP job to complete verification after migrating to a new DB2 version, or to enabling-new-function or new-function mode.

You do not need to complete any other tasks to ensure that these products continue to execute. These products detect when you migrate to a new DB2 version and automatically perform binds to accommodate new columns for the new release.

Note
If you use DB2 data sharing and have members in the data sharing group at different version levels of DB2, run $770IVP on members at the lower level of DB2. For more information, see the IBM parameter ABIND=COEXIST in DSNZPARM.

Migrating from an earlier version of RECOVERY MANAGER

Additional tasks, which are dependent on the versions you are updating from and to, are necessary if you migrating from an earlier version of RECOVERY MANAGER.

System and SQL Performance products and solutions

To maintain the System and SQL Performance products when you migrate to a new version of DB2, follow the steps and guidelines in this procedure.

Before you begin

- To maintain the product when you create a new DB2 catalog for a new version of DB2, perform a full installation of the product. Then you will be operating in exploitation mode.

- Perform this procedure only after you migrate to the new version of DB2 in compatibility mode or NFM mode.
To migrate between versions of DB2

1. Before you migrate to a new version of DB2, stop the DOM agent by issuing the following console command:
   
   ```
   /dbcssid DOM,STOP
   ```

   The `dbcssid` value represents the DBC subsystem ID.

2. Migrate to the new version of DB2.

3. Start the DOM agent by issuing the following console command:
   
   ```
   /dbcssid DOM,START
   ```

4. Set up the Common Explain component:
   
   a. If the names of your DB2 libraries have changed, update the following members to reflect the new names:

<table>
<thead>
<tr>
<th>Member</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSS2ssid</td>
<td>Control members that contain the plan name and DB2 libraries</td>
<td>HLQ.UBMCSAMP</td>
</tr>
<tr>
<td>ACTPSS</td>
<td>Contains the CATALOG MANAGER interface to SQL Explorer</td>
<td>HLQ.UBMCCLIB</td>
</tr>
<tr>
<td>SQLX edit macro</td>
<td>Contains the plan name and library names for explaining a single SQL statement from a program</td>
<td>SYSPROC concatenation</td>
</tr>
</tbody>
</table>

   b. Based on the version of DB2 to which you are migrating, complete the appropriate steps to bind packages and plans:
If you are migrating to this version | Do this
--- | ---
DB2 Version 10 | 1. If SYSIBM.SYSPACKSTMT has not been converted to the new DB2 Version 10 format, rebind all packages by using DAAssidP (bind packages), and bind the plan by running DAAssidB (bind plan) in UBMCSAMP.
2. After SYSIBM.SYSPACKSTMT has been converted, run DAAUP9#A. Then, rebind the plan by running DAAssidB (bind plan) in UBMCSAMP.
3. Convert the user plan tables to Unicode by using sample jobs provided by IBM. These jobs include DSNTIJPM, DSNTIJXA, DSNTIJXB, and DSNTIJXC.

DB2 Versions 11 or 12 | Rebind all packages by using DAAssidP (bind packages), and bind the plan by running DAAssidB (bind plan) in UBMCSAMP.

If Automatic Rebind is set to YES or COEXIST, you do not need to perform the rebind.

Then you will be operating in exploitation mode.

**Earlier DB2 version fallback**

This topic describes the process of returning to an earlier version of DB2.

**Administrative products and solutions**

When you fall back to an earlier version of DB2, you must perform certain tasks to ensure that the Administrative products continue to execute.

**Falling back to DB2 Version 10 from Version 11**

Complete the appropriate procedures to enable the Administrative products to execute after falling back to DB2 Version 10 from DB2 Version 11.

**To enable fallback for ALTER or CHANGE MANAGER version 11.1 or later**

1. To rebind all of the packages and plans, run the following bind jobs from HLQ:UBMCCNTL:
   - ACMssidP
   - ACMssidB
   - ACSssidP
To enable fallback for ALTER, CHANGE MANAGER, or CATALOG MANAGER and catalog indirection

1. To rebind all indirect packages or plans for the earlier version of indirection, run one of the following sets of bind jobs from HLQ.UBMCCNTL:

   Note
   The earlier version of indirection must still exist.

- (ALTER or CHANGE MANAGER) ACMssidZ and ACMssidB
- (CATALOG MANAGER) ACTssidZ
- (CATALOG MANAGER version 11.1.00 and later) PS1ssidZ or DAAssidZ

2. Run AEXssidP from HLQ.UBMCCNTL.

To enable fallback for CATALOG MANAGER version 11.1 or later

1. To rebind all CATALOG MANAGER packages and plans, run the following bind jobs from HLQ.UBMCCNTL:

   - ACTssidP
   - ACTssidB
   - PS1ssidP or DAAssidP
   - PS1ssidB or DAAssidB
   - AEXssidP

To enable fallback for DASD MANAGER PLUS version 11.1 or later

1. To rebind all of the packages and plans, run the following bind jobs from HLQ.UBMCCNTL:

   - ASUssidP
   - ASUssidB
   - ACSssidP
   - ATSssidP
   - AEXssidP
Backup and Recovery products and solutions

When you fall back to an earlier version of DB2, you must perform certain tasks to ensure that the Backup and Recovery products continue to execute.

Falling back to an earlier version of DB2

If fallback to an earlier version of DB2 is necessary for NGT Recover, perform the following procedure:

1. Free the packages contained in the products collection (for example, FREE BMCAFR.* for NGT Recover).
2. Run the $770IVP job to complete the verification procedure.

*Note*
Performing these tasks prevents the possibility of SQLCODE -607 errors that might result when the packages were bound after an upgrade get an automatic rebind after you fall back.

If you use DB2 data sharing and have members in the data sharing group at different version levels of DB2, run $770IVP on members at the lower level of DB2.

For more information, see the IBM parameter ABIND=COEXIST in DSNZPARM.

Utility products

For the Utility products, run the $770IVP job to complete verification after falling back to an earlier version of DB2.

System and SQL Performance products and solutions

To maintain the System and SQL Performance Products when you fall back to a previous version of DB2, follow the steps and guidelines in this procedure.

To fall back to a previous version

1. If the names of your DB2 libraries have changed, update the following members to reflect the name of the previous version of the libraries:
<table>
<thead>
<tr>
<th>Member</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSS2ssid</td>
<td>Control members that contain the plan name and DB2 libraries</td>
<td>HLQ.UBMCSAMP</td>
</tr>
<tr>
<td>ACTPSS</td>
<td>Contains the CATALOG MANAGER interface to SQL Explorer</td>
<td>HLQ.UBMCCLIB</td>
</tr>
<tr>
<td>SQLX edit macro</td>
<td>Contains the plan name and library names for explaining a single SQL statement from a program</td>
<td>SYSPROC concatenation</td>
</tr>
</tbody>
</table>

2 *(falling back from DB2 Version 10)* If SYSIBM.SYSPACKSTMT has reverted to the non-Version 10 format, free PG PSS0SQL.

3 If Automatic Rebind (ABIND) is set to **NO** on your subsystem, rebind all packages by using DAAssidP (bind packages) and then bind the plan by running DAAssidB (bind plan) in UBMCSAMP. The ssid value represents the subsystem ID. (If Automatic Rebind is set to **YES** or **COEXIST**, you do not need to perform the rebind.)
Index

[Bind] parameters
  APOOWNER [Bind parameters: APOOWNER] 135
  AuthID [Bind parameters: AuthID] 135
  BindOwner [Bind parameters: BindOwner] 135
*DATA, modifying in BMCDB2 CLIST 170
*PROD, modifying in BMCDB2 CLIST 171
 //NGTUSTEP 350
&SYSCLONE symbolic 281
&SYSCLONE symbolic variable 286
#DEFHFS member of UIM server sample library 320
#LOADHFS member of UIM server sample library 320
#NORMAL member of UIM server sample library 316
#UIMX member of UIM server sample library 317
$230VSAM job 286
$465INIT job 270
$480INIT job 230, 296
$725ALOC installation job 307
$725ALOC job 307
$730DOPT customization job 146
$730DOPT job 146, 309
$740ALTR job 362
$740INST job 194
$770IVP customization job
  running after installation 328
$770IVP job 328, 329, 361, 365
$781PERF job 339, 344, 348
$DOM substitution symbols 254
$DOMARC job 270
$DOMARCN job 270
$DOMDATE job 270
$DOMDSN job 270
$DOMLSET job 270
$DOMPLX job 270
$DOMSSN job 270
$DOMTIME job 270
$SUBSTR (substrings in copy job) 254

9DEFAULT profile 266

A
abend code of U0008 307
abends
  preventing 148
above-the-bar storage 143
ACCESS parameter 216
access, controlling
  in CHECK PLUS 82
  in LOADPLUS 84
  in REORG PLUS 88
  in UNLOAD PLUS 91
XIM 203
accessing multiple z/OS systems 315
ACF2. See CA ACF2
ACF2/RACF 136
ACMFRONT program 216
ACP product code 167
ACTCSQBU package 151
ACTDCL command 193
ACTEMAIN command 193
ACTEMAIN program 216
action POF 323
ACTIVATE command 207
activating XIM initiators 207
ACTJTEQ package 190
ACTPSS CLIST 161, 211
ACTQLBH package 151
adding products, BMCDB2PR panel 167
ADDLOAD1 POF keyword 151, 153, 154
ADDLOAD2 POF keyword 151, 153, 154
Administrative products
  migrating to a new version of DB2 355
AEXADMF1 CLIST 178, 190, 211
AEXADMF2 CLIST 178, 190, 211
AEXAUNLD package 100
AEXvrmDA Execution Monitor Entry plan 99
AEXvrmDM Execution Monitor plan 100
AFF_TIMEOUT_SECS option 309
affinity timeout, changing 309
agent
  DOM 103
AJX#DSNS member 165
AJX#USRV member 165
AJXCOMPS member 165
AJXSTEU SLIB member 151, 153, 154
alias qualifiers
  using for catalog indirection 185
aliases
  overview 185
allocating
  installation options module, in BMCDB2 CLIST 177
allocation 307
ALLOW_NETCMD option 317
ALM product code 167
ALP product code 167
ALTCLIST variable 214
ALTER
  BMC Software Utilities interface 153
  BMCALTER command 178
  Fast Path Navigation 178
  installation options processing 184
  program name 216
  upgrading to CHANGE MANAGER 169
  using catalog indirection 182
  using DASD MANAGER PLUS 156
ALTER authority 84, 88
ALTER privileges 84
ALTFRONT program 216
ALTLIB command 214
ALUFront program 216
ALUWLDDL CLIST 211
ALUXGRNT CLIST 211
APF
  DASD 101
APF authorizations
  High-speed Apply Engine 136
  Log Master for DB2 115
  NGT Copy 94
  NGT Recover 98
  R+/CHANGE ACCum 119
  RECOVERY MANAGER 96
APF-authorized 139
APF-authorized load library 328
APF-authorized load library, sharing 163
APFONLIN installation option 115
APOWNER parameter 135
APPLDEV rules 301
application ID, modifying in BMCDB2 CLIST 176
APPTUNE for DB2
  generating Help text from DB2 trace records 237
  issuing a dynamic Explain command 336
  plan name 105
  report log data sets 106
  restricting authority 111
  verifying the installation 266
  verifying the product for data sharing members 233
APPTUNE product code 167
APTGRANT member of DBSAMP 84
Archive History file
  access 116
ARM product code 167
ARMSSOPTS 224
ARMBSRR batch job 223
ASQ product code 167
ASU_XP_UIMSRVHOST POF keyword 198
ASU_XP_UIMSRVPORT POF keyword 198
ASUDOPT installation option 156
ASUFMAIN program 216
ASUVERSN member of DASD MANAGER PLUS load library 156
ASUvrmDJ BMCTRIG Utility Job Generation plan 99
ASUvrmDR Report Display plan 99
ASUvrmDS Statistics Collection plan 99
AUTH_TIMEOUT_SECS option 309, 317
authexpl 102
authorization
  MONITOR2 88
  timeout for 309, 317
authorizations 82, 139

368  BMC Products and Solutions for DB2 Customization Guide
ALTER 84
ALTER authority 88
ALTER privileges 84
APF
    SMS service routine load library 328
BINDADD 84
CONTROL 84
CONTROL authority 88
CREATE 84
DB2 and data set  
    CHECK PLUS 82
    LOADPLUS 84
    REORG PLUS 88
    UNLOAD PLUS 91
DBADM 88
DBCTRL 88
DISPLAY 88
    High-speed Apply Engine 128
INSERT 84
INSTALL SYSADM authority 84
LOADPLUS 84
Log Master for DB2 114
mechanisms, description 82
needed to execute REORG PLUS 88
NGT Copy 93
NGT Recover 97
PACLOG 116
R+/CHANGE ACCUM 118
RACF 88
    CHECK PLUS 82
    LOADPLUS 84
    UNLOAD PLUS 91
READ 82
READ privileges 84
RECOVERY MANAGER 95
required for canceling threads 88
required for checking referential constraints 84
required for DEFINE NO data sets 84
required for loading tables with identity columns 84
required for XML reorganizations 88
required to run CHECK PLUS 82
required to run SQLAPPLY load 84
system 84, 89
TRACE 88
UNLOAD PLUS 91
UPDATE 84
verifying 81, 82

B
BASEID parameter 216
BBPARM parameter set (PAP) 107
BCSS commands, PACLOG 225
BDOPTS installation option 158
BindOwner parameter 135
AuthID parameter 135
bind jobs 146
BIND PACKAGE options, CATALOG MANAGER 190
BindAction parameter 132
BINDADD authority
    DB2 131
BINDADD privileges 84
binding packages and plans 163
BINDOWN installation option 114
BindOwner parameter 132
block size 308
BMC Archive History file  
    access 116
BMC Software Utilities, interacting with  
    ALTER 153
    CATALOG MANAGER 151
    CHANGE MANAGER 153
BMC Workbench  
    plan name 105
    requirements 294
BMC Workbench repository 297
BMC_CHECK_LOAD POF keyword 151, 153
BMC_COPY_LOAD POF keyword 151, 153, 154
BMC_LOAD_LOAD POF keyword 151, 153, 154
BMC_RECOVER_LOAD POF keyword 151, 153
BMC_REORG_LOAD POF keyword 151, 153, 154
BMC_UNLOAD_LOAD POF keyword 151, 153
BMC_UTIL_SYNC synonym 151
BMC.Utility synonym 151
BMCALTER command 178
BMCCAT command 178
BMCHG command 178
BMCDASD command 178
BMCDDB2 CLIST

Index 369
adding a product 170–173
allocating indirect installation options module 184
allocating installation options module 177
BMCDB2C variable 214
BMCDB2P variable 214
BMCDB2T variable 215
CONTAB command 327
editing 214
editing variables 214
enable 211
GENTABLE variable 214
improving performance 214
installation 213
invoking explicitly 215
invoking implicitly 215
invoking session profile command 191
ISPF interface considerations 213
modifying control table 170–173
restricting users from CATALOG MANAGER functionality 187
setting locking options 190
specifying an entry panel 188
supporting catalog indirection 178
supporting subsequent DB2 subsystems 177
updating with member BMCDB2CI 178
updating with member BMCDB2SS 177
using DASD MANAGER PLUS within ALTER or CHANGE MANAGER 156
using DASD MANAGER PLUS within CATALOG MANAGER 158
BMCDB2 command 216
BMCDB2C variable 214
BMCDB2CI member 178
BMCDB2H panel
generating 214
BMCDB2P variable 214
BMCDB2P2 panel
DB2 SSID field 215
generating 214
BMCDB2PR panel 167
adding Indirect option 169
adding products 167
bypassing 216
changing ALTER to CHANGE MANAGER 169
DB2 SSID field 215
generating 214
BMCDB2PR panel, generated interface 213
BMCDB2SS member 177
BMCDB2T variable 215
BMCDB2TB panel
generating 214
verifying 327
BMCDBRVIC CLIST 211
BMCGUIPL 101
BMCHIST table
CATALOG MANAGER synonym 151
BMCSYNC table
CATALOG MANAGER synonym 151
BMCUTIL table
CATALOG MANAGER synonym 151
BMIIDB2XA member 163
BMIIDB2XB member 163

C

CA ACF2 authorizations
R+/CHANGE ACCUM 119
CA ACF2 security product 82
CA Top Secret security product 82
CA-ACF2 101
CA-ACF2 authorizations
PACLOG 116
CA-ACF2 security 120
CA-ACF2 security PACLOG 116
CA-ACF2 security required 88
CA-Top Secret 101
CA-Top Secret security 121
Call Attach Facility, testing(PSS/AFD) 343
canceling threads
authorizations required 88
CAP product code 167
CAT3 prefix 185
catalog contention, reducing 186
catalog copy, using for catalog indirection 186
catalog indirection
customizing the interface 169
implementing 183
improving performance 163
ISPF interface considerations 169
maintaining 183
overview 182
post-installation considerations 169
supported by member BMCDB2CI 178
CATALOG MANAGER
BIND PACKAGE options 190
BMC Software Utilities interface 151
BMCCAT command 178
CONNECT command 192
CURRENTDATA value 190
customizing CLISTs 234
entry panel 188
Fast Path Navigation 178
generating DDF aliases 193
initial command 187
installation options processing 184
invoking session profile command 191
ISOLATION level 190
locking options command 190
product log tables 187
program name 216
SEARCH command 186
setting locking options 190
SPACE command 158
STATS command 158
using catalog indirection 182
using DASD MANAGER PLUS 156, 158
using SQL Explorer 161
catalog tuning 186
CDBSS 308
CFUNC parameter 216
CHANGE ACCUMULATION PLUS product code 167

CHANGE MANAGER
BMC Software Utilities interface 153
BMCCHG command 178
Fast Path Navigation 178
generating DDF aliases 193
installation options processing 184
program name 216
upgrading from ALTER 169
using catalog indirection 182
using DASD MANAGER PLUS 156

CHECK PLUS
authorizations needed 82
catalog tuning 186
CHECK PLUS
authorizations needed 82

checkpoint data set 307
CQSNUM CLIST 211
class, security 122, 125
CLIST
ACTPSS (PSS/AFD) 234
customize for SQL Explorer and CATALOG MANAGER (PSS/AFD) 234
re-blocking (DDT) 273
re-blocking (PAP) 240

CLISTs
ACTPSS 161
AEXADMF2 190
data sharing environments 287
enabling 212
invoking 215
list of 211
UPDTBMC 167
XBM 279
CLOSE cursor command in PSSRXSQL 304
CLSTEXEC parameter 216
collection ID, in product bind job 146
CollectionID parameter 132
comment command 288
COMMIT command in PSSRXSQL 304
COMMNDXX member of SYS1.PARMLIB 308
common connection list 196
Common SQL
upgrading shared component 163
compiling the SLIB 165
CONFIG parameter 281
configuration member for UIM server
creating 316
configuration parameters, by name
APOWNER 135
AuthID [Bind] 135
BindOwner [Bind] 135
CONNECT command 327
constraints, referential, authorization for checking 84
CONTAB command 327
CONTROL authority 84, 88
control table
adding a product 170
allocating application ID 176
editing CATALOG MANAGER servers 192
locating 170
modifying 170
modifying in the BMCDB2 CLIST 170–173
modifying the application ID 176
updating with member BMCDB2SS 177
controlling access
in CHECK PLUS 82
in LOADPLUS 84
in REORG PLUS 88
in UNLOAD PLUS 91
to DASD MANAGER PLUS 98
XIM 203
conventions, documentation 11
copies, encrypted, authorization requirements 91
COPY 140
Index

DBC 293
  and Recovery Management 223
  and RECOVERY MANAGER 223
DBC agents 293
DBC security 103
DBCS$Tc job 238
DBDBRM library 165
DBRMLIB DD statement 165
DCC$VARS data set (PAP) 106
DD statements
  XBMREPnn 285
  XBMXINIT 285
  XBMXTASK 285
DDF (Distributed Data Facility) 193
DDT product code 167
decimal format (global options) 266
default options. See installation options
DEFAULT rules 301
DEFAULT security profile (DDT/SPD) 275
DEFAULT user profile (DDT/SPD) 275
DEFINE NO, objects created with authorization required 84
deployment
  displaying names of profile data sets and JCL libraries 211
dispatching priority
  OPERTUNE 271
DISPLAY privileges 84, 88, 91
Distributed Data Facility. See DDF
Distributed Data Facility, testing (PSS/AFD) 346
documentation information 13
DOM agent 103
DOMBCOPY (copy trace data set)
  substitution symbols (PAP) 254
DOMESL0 (PAP) 227
DOMEXIT1 104
DOMEXIT2 (PAP) 111
DOMEXIT4 (PAP) 111
DOMPLEX Profile (PAP) 247
  adding a subsystem 236, 251
  Administration menu 249
  check the DB2 subsystems 236, 251
  check the output groups 254
  checking the values 249
  DOMPLEX Profile Administration menu 249
  DOMPLEX Profile Menu 249
DOMPOST 270
DOMRBLK (PAP) 240
DSNAME 350
DSNW133I messages (PAP) 330
dynamic SQL 187

E
ELO locking option 190
EMC Symmetrix Control Facility 289
EMC Symmetrix devices
  required software 289
EMC TimeFinder 289, 290
enabling
  REXX executables 195
enabling DDF 193
enabling interaction between Log Master and RECOVERY MANAGER 160
enabling interaction between NGT Copy and RMGR 161
enabling interaction between NGT Recover and RECOVERY MANAGER 160
encrypted copies, authorization requirements 91
enterprise connection list 196
entry panel command in CATALOG MANAGER 188
ENVI command 180, 327
error messages
  PSSRXSQL 305
examples
  allocating a dump data set (DDT) 277
examples, resource security profile
  CA-ACF2 120
  CA-Top Secret 121
  RACF 124
EXCPs 308
EXECUTE authority 138
EXECUTE command in PSSRXSQL 304
EXECUTE privileges
  CHECK PLUS 82
  High-speed Apply 84
  LOADPLUS 84
  REORG PLUS 88
  UNLOAD PLUS 91
executing CLISTs 212
Execution Monitor shared component 163
Execution plans, names and descriptions 99
exits
  security 82
exits, user
  authorizations for 88
expert rule variable 301
expert rules
defined 300
overview 300
Explain Object Specification panel (BDS/ASQ/AFD) 336
Explain or Execute Parameters panel (BDS/ASQ/AFD) 336
Explain Results panel (BDS/ASQ/AFD) 336
Export
ASU_XP_UIMSRVHOST POF keyword 198
ASU_XP_UIMSRVFPORT POF keyword 198
POF keywords 197
SAF authority 198
setting the primary UIM server host name 198
setting the primary UIM server port 198
EXTENDED BUFFER MANAGER (XBM)
REORG PLUS requirements 88
EXTENDED BUFFER MANAGER product code 167
external functions
PSSRXSQL 304

F
facility class, RACF security 125
Facility class, RACF security 122
fallback to an earlier version of DB2 363
falling back to an earlier version of DB2
  Administrative products 363
  Backup and Recovery products 365
falling back to an earlier version of DB2, Backup
  and Recovery products 365
falling back to DB2 Version 10, from Version 11 363
Fast Path Navigation
  commands 178
  enabling locking options 190
FIXSQNUM CLIST 211
FlashCopy
  PROIGN DD statement 285

G
GDGs (generation data groups)
  generating JCL 165
  specifying 166
GENERATE command 170, 192, 215
  generating an archive 269
  generating DDF aliases 193
  generating JCL
  generation data groups 166
  product 165
  REGION statements 165
generation data groups. See GDGs
GENTABLE variable 170, 192, 214
  granting authorizations 82
  granting privileges to PUBLIC 88
group attatch name 172
GUDOPT 298

H
HELP data set (PAP) 106
HFS data set 319, 320
HFS_DATASET option 317
High-speed Apply Engine
  APF authorizations 136
  authorizations 84
  DB2 authorizations 129
High-speed Apply Engine user authorizations 128
history table (BMCHIST)
  CATALOG MANAGER synonym 151
Hitachi devices
  required software 289
  HLQ_UBMCCNTL members
    BMIDB2XA 163
    BMIDB2XB 163
    T1S#ACTU 151
host connection 196
HPLAN installation option 151

I
IBM Enterprise Storage Subsystem (Shark) devices
  required software 289
IBM Storage Management Subsystem. See SMS
ICF (Integrated Catalog Facility) 88
  identity columns, authorization required 84
  idle timeout, changing 309
IDs
  RACF 82, 91
  IEFUSI exit 143
Impact Analysis Object Specification panel (PSS/ASQ/AFD) 345
  improving performance 163, 214
IMS component
  disabling 281
inactivating XIM initiators 206
Index Term 38, 44, 46, 50, 61, 66, 71, 109, 139, 307, 355
indexes

authorization 84
XML 88

indexes, creating 163

Indirect option 169

initiator procedure, XIM 202

INSERT privileges 84

INSTALL SYSADM authority 84

installation considerations

generating ISPF interfaces 213
using catalog indirection 182

installation options

APFONLIN 115
BINDOWN 114
OPNDB2ID 94, 116
READONLY 94
refreshing 180
sharing among DB2 subsystems 175

installation options module

specifying for catalog indirection 184

Installation Systems

CLISTs 211

installation verification procedure. See IVP

Instant Snapshot copy, system authority needed 91

interaction

ALTER with BMC Software Utilities 153
ALTER with DASD MANAGER PLUS 156
CATALOG MANAGER with BMC Software Utilities 151
CATALOG MANAGER with DASD MANAGER PLUS 158
CHANGE MANAGER with BMC Software Utilities 153
CHANGE MANAGER with DASD MANAGER PLUS 156
DASD MANAGER PLUS with ALTER 156
DASD MANAGER PLUS with BMC Software Utilities 154
DASD MANAGER PLUS with CATALOG MANAGER 158
DASD MANAGER PLUS with CHANGE MANAGER 156

interaction between

NGT Copy and DASD MANAGER PLUS 154
interaction between Log Master and RECOVERY MANAGER 160

interaction between NGT Copy and RMGR 161

interaction between NGT Recover and RECOVERY MANAGER 160

ISOLATION value, CATALOG MANAGER 190

ISPF interface considerations
catalog indirection 169

ISPF-Export
configuring 195

IVP (installation verification procedure) 328
Administrative products 327

J

JCL Generation POF
creating additional POFs 323

JCL Generation shared component 163

JCL libraries

viewing during installation 211

JCL, generating

environment specific 165
for generation data groups 166
REGION statements 165

JES job log

OPERTUNE 276

System and SQL Performance products 330

Join sysplex group when PSS started option 281

L

LGC 293

and Recovery Management 223

and RECOVERY MANAGER 223

LGCOMAIN 101

LIBDEF facility 216

LIBDEF parameter 216

libraries, XBM 286

Linklist Lookaside (LLA) (PAP) 246

LOAD RESUME YES SHRLEVEL CHANGE SQLAPPLY, authorizations for 84

LOADEXEC parameter 216

LOADLDEF parameter 216

LOADPLUS

authorizations needed 84
locking options 190

Log Master

APF authorizations 115

DB2 authorizations 114

interaction with RECOVERY MANAGER 160

RACF authorizations 116

user authorizations 114

Log Master product code 167
M

macros
  UPDTDB2 167
main menu
  common (PAP) 227
maintenance
  applying to control access 140
MainView for DB2
  generating help text from DB2 trace records 237
MainView for DB2 - Data Collector
  issuing a dynamic Explain command 336
  verifying the installation 266
MainView for DB2 \xd0 Data Collector (BDS)
  invoking 227
MainView SRM StopX37 product 148
MASTERJB 350
materializing DEFINE NO data sets
  authorization required 84
Max log buffers 232
Max read buffers 232
MEMLIMIT system parameter 143, 328
menu
  making products available 243
messages
  (DSNW133I) (PAP) 330
migrating
  data 81
migrating the Administrative products and solutions 355
migrating to a new version of DB2
  Backup and Recovery products 361
  Utility products 361
migrating to DB2 Version 10 from Version 9 new-function mode 358
migrating to DB2 Version 11 from Version 10 new-function mode 356
migration
  RECOVERY MANAGER 361
modifying MVS image variables 207
MONITOR2 authority 88
MS parameter 281
multiple
  MVS systems, accessing multiple 315
  z/OS systems, accessing 315
multiple UIM servers 316
MVS image variables 207
MVS security (PAP) 106

N

naming conventions
  catalog indirection 184
network browser command interface, enabling or disabling 317
new DB2 version migration 355
NGLARCH 269
  renaming 270
NGT Copy 94
  APF authorizations 94
  DB2 authorizations 93
  enabling interaction with DASD MANAGER PLUS 154
  interaction with RMGR 161
  product code 167
  RACF authorizations 94
  user authorizations 93
NGT Load 136
NGT Recover
  APF authorizations 98
  DB2 authorizations 97
  interaction with RECOVERY MANAGER 160
  user authorizations 97
NGTCKPT 307

O

OMVS segment for RECOVERY MANAGER 95
OPEN cursor command in PSSRXSQL 304
OPENTBL parameter 215, 216
operator user profile (DDT/SPD) 275
OPERTUNE for DB2
  CLIST 273
  CLIST re-blocking 273
  DDTOPER user profile 275
  DEFAULT security profile 275
  DEFAULT user profile 275
  dispatching priority 271
  security 275
  started task 276
  system profile 276
OPERTUNE product code 167
OPNDB2ID installation option 82, 94, 116
OPNDB2ID installation option, effects on RACF authorizations 91
OPNDB2ID option
effects on RACF authorizations 88
option sets 298
options
  modifying 146, 309
  UIM 309

P

packages
  ACTCSQBU 151
  ACTJTEQ 190
  ACTQLBH 151
  binding 163
  CHECK PLUS 82
  LOADPLUS 84
  REORG PLUS 88
  UNLOAD PLUS 91

PACLOG
  access to the BMC Archive History file 116
  BCSS commands 225
  CA-ACF2 authorizations 116
  interacting with RECOVERY MANAGER 161
  RACF authorizations 116
  system security authorizations 116
  user authorizations 116

PACLOG product code 167

Parallel Sysplex Support (PSS) component
  disabling 281
  setting up 290
  XBMGROUP name 281

parameters
  ACCESS 216
  CFUNC 216
  CLSTEXEC 216
  LIBDEF 216
  LOADEXEC 216
  LOADLDEF 216
  MEMLIMIT 143
  OPENTBL 215, 216
  PGM 216
  PROD 216
  SHRAPP 216
  SSID 216
  system 143

parent table indexes, authorization for 84
PARM 350
PARMLIB TSO command 115
PCPY1_PREFIX POF keyword 166
PCPY2_PREFIX POF keyword 166

performance
  improving 185

personal connection list 196

PGM parameter 216

PKLIST statement, in product bind job 146

plan(PAP) 101, 105

PlanName parameter 132

plans
  binding 163
  CHECK PLUS 82
  DASD MANAGER PLUS 99
  LOADPLUS 84
  REORG PLUS 88
  UNLOAD PLUS 91
  variables 98

PMD$HIST data set (PMD/SPD) 106

POF (product options file)
  user 323

POF (product options file), JCL Generation
  creating additional POFs 323

POF keywords for Export 197

POF values, refreshing in the user profile 181

POFRESET CLIST 211

Pool Advisor for DB2
  checking the system console log messages 330
  BBPARM and BBTMPLT data sets 107
  data sets 107
  generating help text from DB2 trace records 237
  starting a session 349
  verifying the installation 266

ports
  number for UIM server 309
  UIM server 317

preparing for large archive logs
  RECOVERY MANAGER 222

preventing x37 abends 148

privileges
  ALTER 84
  See also authorizations

PROC command file 288

PROD parameter 216

product authorizations
  verifying 81

product log tables, accessing 187

product options file. See POF

products
  binding to shared components 163
  JCL, generating 165

PROFILE data set (PAP) 106

profile data sets
viewing during installation 211
profiles
naming convention 122, 125
security 122, 125
PROIGN DD statement 285
PSSRXSQL external function 304
PUBLIC, granting to 88
publications, related 13

Q
qualifier status, USED/REUSE 185
QUICKEXIT 307
QUIESCE command 206

R
R+/CHANGE ACCUM
APF authorizations 119
CA ACF2 authorizations 119
DB2 authorizations 118
MODIFY ACCUM command 119
RACF authorizations 119
user authorizations 118
RACF 84, 101
authority needed to execute CHECK PLUS 82
DASD 100
OPNDB2ID option 82
security exit 82
RACF (IBM Resource Access Control Facility)
creating general resource profiles 140
RACF (IBM Resource Access Control Facility)
authority 88
CHECK PLUS 82
LOADPLUS 84
UNLOAD PLUS 91
RACF authority (PAP) 107
RACF authorizations
Log Master 116
PACLOG 116
R+/CHANGE ACCUM 119
RCPY1_PREFIX POF keyword 166
RCPY2_PREFIX POF keyword 166
READ privileges
CHECK PLUS 82
LOADPLUS 84
READONLY installation option 94
Recovery Management
and DBC 223
and LGC 223
RECOVERY MANAGER
and DBC 223
and LGC 223
APF authorizations 96
creating temporary tables 221
customizing 221
DB2 authorizations 96
interacting with PACLOG 161
interaction with Log Master 160
interaction with NGT Copy 161
interaction with NGT Recover 160
migrating from an earlier version 361
migrating to data sharing 222
OMVS segment 95
preparing for large archive logs 222
RACF authorization 95
restricting TSO commands 97
setting up data sharing 222
system security authorizations 95
user authorizations 95
RECOVERY MANAGER (for DB2)
archive history file 223
option set 224
packages 224
repository 224
RECOVERY MANAGER product code 167
referential constraints, authorization for checking 84
refresh, unsuccessful 180
refreshing user options 180
REGION parameter 165, 285
REGION statements, generating JCL 165
related publications 13
renaming NGLARCH 270
REORG_HISTORY synonym 151
Resource Access Control Facility. See RACF
Resource Access Control Facility (RACF)
RACF resource profiles 122, 125
RACF user ID 122
user authorizations for XBM 120, 122
restricting access
applying a zap 140
specifying a resource profile 140
to parallelism feature 140
restricting TSO commands for RECOVERY
MANAGER 97
return codes
PSSRXSQL 305
REXX exec 301
REXX executables
  implicitly executing for DASD MANAGER PLUS 195
ROLLBACK command in PSSRXSQL 304
RTCS 293
rules 300
  APPLDEV 301
  DEFAULT 301
  editing 302
  predefined 301
rules engine 301
ruleset 301
Run authorized 102

S
SAF authority for Export 198
sample library, UIM
  #DEFHFS member 320
  #NORMAL member 316
  #UIMX member 317
SCCAUTH program, authorization 96
SEARCH command
  CATALOG MANAGER 186
security
  CHECK PLUS 82
  class 122, 125
  exit 82
  LOADPLUS 84
  objects 187
  OPERTUNE for DB2 275
  product (PAP) 111
  profile 122, 125
  REORG PLUS 88
  SECURITY data set (PAP) 106
  using packages other than RACF 91
  using RACF 91
  verification 82
security authorization timeout 309, 317
SELECT 140
SELECT authority
  LOADPLUS 84
SELECT privileges 88
server configuration
  UIM 199
server-side storage data set 309
servers, CATALOG MANAGER 192
session profiles 191
shared components 163
shared components, binding a product to 165
sharing installation options 175
SHRAPPL parameter 216
SHUTDOWN command 207
shutting down XIM 207
SIBBATCH program 290
single UIM server for multiple products 323
SLIB data set
  compiling 165
  editing 165
  testing 165
SMF$DHSP 199
SMFPRM member 143
SMS information 350
SMS-managed data sets 328
SPACE command, CATALOG MANAGER 158
SQL Explorer
  integrating with CATALOG MANAGER 161, 211
  testing the Call Attach facility 343
SQL Explorer for DB2
  customizing CLISTs 234
  plan name 105
  testing impact analysis 345
  testing the distributed data facility 346
  verifying installation 342
  verifying the installation 266
  verifying the product for data sharing members 233
SQL Performance for DB2
  plan name 105
  report log data sets 106
  restricting authority 111
  verifying the installation 266
  verifying the product for data sharing members 233
SQLX edit macro (PSS/AFD) 234
SSID parameter 216
SSID, making profile unique 176
STAGEDSN option
  authority needed 88
started tasks
  procedure for UIM server 317
  UIM server 317
starting
  UIM server 309
starting XIM 205
startup member, UIM server
changing options 309
creating 316
STATS command, CATALOG MANAGER 158
status
of XIM, determining 205
STATUS command 205
stopping
UIM server 309
StopX37 product 148
Storage Systems Integration (SSI) component
disabling 281
setting up 289
storage, virtual 143
substitution symbols, $DOM (ASQ/AFD) 254
SUBSTR function 270
substrings (DOMBCOPY) 254
subsystem profile (DDT/SPD) 276
supporting subsequent DB2 subsystems, in
BMCDB2 CLIST 177
symbols, $DOM (ASQ/AFD) 254
synonyms
used by CATALOG MANAGER 151
SYS parameter 281
SYS1.PARMLIB data set 115
SYS3 136
SYSADM 138, 140
SYSADM authorization 139
SYSCTL 138
SYSCTRL 140
SYSEXEC concatenation, enabling REXX
executables 195
SYSIBM.SYSSEQUENCES table 84, 88
SYSIBM.SYSSEQUENCESDEP table 84, 88
SYSIBM.SYSXMLRELS table 88
SYSIN 350
SYSLMOD DD statement 180
SYSPRINT messages
OPERTUNE 276
System and SQL Performance products 330
System and SQL Performance products
data sets 106
Installation Assistant 233
plan 105
refreshing the Linklist Lookaside 246
security
DB2 103
RACF 107
System and SQL Performance products
CA-ACF2 authority (PAP) 107
security
CA-ACF2 107
CA-ACF2 (PAP) 107
RACF (PAP) 107
System and SQL Performance products
CA-ACF2 authorization 107
RACF authority 107
verify/change global options 262
verifying/changing global resource enqueues 244
System and SQL Performance products generating
Help text 237
system authorization
verification 82
System Authorization Facility (SAF) 120, 121
System Authorization Facility (SAF) for Export 198
System Display and Search Facility (SDSF) 120
System Performance for DB2
BBPARM and BBTMPLT data sets 107
checking the system console log messages 330
generating Help text from DB2 trace records 237
starting a session 349
verifying the installation 266
system security authorizations
PACLOG 116
RECOVERY MANAGER 95

T
T1S#ACTU member 151
T1S#CDBS member 193
table privileges
DB2 129
tasks
editing rules 302
TEMPLATE data set (PAP) 107
temporary objects used in IVP 328
temporary tables
RECOVERY MANAGER 221
threads, canceling
  authorizations required 88
timeout feature, UIM server 309
timeout, affinity 309
Top Secret. See CA Top Secret
TRACE authority 88
trace data sets (PAP)
  description 106
TRACE member for UIM server
tracing, UIM server 309
troubleshooting, execution of XIM 210
tuning, catalog 186

U

UBMCCNTL data set, BIND packages and plans
  165
UIM 293
UIM server
  #DEFHFS member of sample library 320
  #NORMAL member of sample library 316
  #UIMX member of sample library 317
affinity timeout 309
changing options 309
creating multiple 316
creating started task procedure 317
HFS data set 309
merging for multiple producets 323
  multiple 316
port number 309
security authorization timeout 309
server-side storage data set 309
single, for multiple products 323
started task 317
starting 309
startup configuration member 309, 316
stopping 309
  TRACE member
  tracing option 309
UIM server configuration 199
UIM server sample library
  #DEFHFS member 320
UIM server sample library:#NORMAL member
  #NORMAL member 316
UIM server sample library:#UIMX member
  #UIMX member 317
UNLOAD PLUS
  authorizations needed 91
unsuccessful refresh 180

UPDATE authority 84
UPDTBMC CLIST 167
UPDTDB2 macro 167
user authorizations
  High-speed Apply Engine 128
  Log Master for DB2 114
  NGT Copy 93
  NGT Recover 97
  PACLOG 116
  R+/CHANGE ACCUM 118
  RECOVERY MANAGER 95
user exits
  authorizations for 88
  security 127
user options
  overlay, avoiding 176
  refreshing 180
  troubleshooting 180
user POF 323
user profile
  OPERTUNE DEFAULT 275

V

variables
  editing in BMCDB2 CLIST 214
  GENTABLE 170, 192, 214
VCAT variable 172
verifying
  authorization 82
  installation 327
  installation (IVP) 328
  product authorization 81
verifying installation
  APPTUNE 336
  Pool Advisor 349
  SQL Explorer 342
virtual storage 143
VSAM component
  disabling 281
VSAM data sets 350

W

warnings
  deleting the 9DEFAULT profile (PAP) 266
Workbench. See BMC Workbench
XBM cataloged procedure 280, 288
XBM initialization command file 288
XBM ISPF interface 279
XBM PROC 279, 286
XBM product code 167
XBM security
  CA-Top Secret 121
  profile 122, 125
XBM subsystems
  multiple 286
  started task 280
XBM$OPTS member 279, 287
XBMGROUP parameter
  defined 281
  parameter in PROC 281
XBMID parameter 281
XBMREPnn DD statement 285
XBMSSID subsystem name 281
XBMXAEX1, XBM security user exit 127
XBMXAEX2, XBM security user exit 128
XBMXINIT DD statement 285, 288
XBMXTASK DD statement 285
XCF_GROUP parameter 207
 XML data, authorizations 88
 XML indexes, authorizations for reorganizing 88
 XPSS parameter 281
 XSSI parameter 281
 XVSAM parameter 281

XIM (Cross-System Image Manager)
  controlling execution 203
  determining status 205
  initiator procedure 202
  modifying active initiators 207
  shutting down 207
  starting 205
XIM commands
  ACTIVATE 207
  QUIESCE 206
  SHUTDOWN 207
  STATUS 205
XIM initiators
  activating 207
  inactivating 206
XIM_GROUP parameter 207
XIMACM started task 205
XIMS parameter 281
Z

z/OS systems, accessing multiple 315