SYBASE®

Authorization Guide

e-Biz Impact™

5.4.5

DOCUMENT ID: DC10094-01-0545-01

LAST REVISED: July 2005

Sybase, Inc., One Sybase Drive, Dublin, CA 94568.

Contents

About This Book

Audience

This book is for security officers and system administrators who are responsible for the configuration of e-Biz Impact security.

How to use this book

This book contains these chapters:

- Chapter 1, “Overview,”provides an overview of e-Biz Impact role-based security and lists the steps necessary to implement authorization for cluster objects.
- Chapter 2, “Configuring Security Database Connections”explains how to configure connections to the Adaptive Server Anywhere database where e-Biz Impact security data is stored.
- Chapter 3, “Setting Up Role-Based Authorization” describes how to set up and assign the appropriate permissions and roles for a cluster.

Related documents

e-Biz Impact documentation The following documents are available on the Sybase™ Getting Started CD in the e-Biz Impact 5.4.5 product container:

- The e-Biz Impact installation guide explains how to install the e-Biz Impact software.
- The e-Biz Impact release bulletin contains last-minute information not documented elsewhere.

e-Biz Impact online documentation The following e-Biz Impact documents are available in PDF and DynaText format on the e-Biz Impact 5.4.5 SyBooks CD:

- The *e-Biz Impact Application Guide* provides information about the different types of applications you create and use in an e-Biz Impact implementation.
- The *e-Biz Impact Authorization Guide* (this book) explains how to configure e-Biz Impact security.
- *e-Biz Impact Command Line Tools Guide* describes how to execute e-Biz Impact functionality from a command line.
- The *e-Biz Impact Configurator Guide* explains how to configure e-Biz Impact using the Configurator.

- The *e-Biz Impact Feature Guide* describes new features, documentation updates, and fixed bugs in this version of e-Biz Impact.
- The *e-Biz Impact Getting Started Guide* provides information to help you quickly become familiar with e-Biz Impact.
- The *Monitoring e-Biz Impact* explains how to use the Global Console, the Event Monitor, and alerts to monitor e-Biz Impact transactions and events. It also describes how e-Biz Impact uses the standard Simple Network Management Protocol (SNMP).
- *Java Support in e-Biz Impact* describes the Java support available in e-Biz Impact 5.4.5.
- The *e-Biz Impact MSG-IDE Guide* describes MSG-IDE terminology and explains basic concepts that are used to build Object Definition Language (ODL) applications.
- The *e-Biz Impact ODL Guide* provides a reference to Object Definition Language (ODL) functions and objects. ODL is a high-level programming language that lets the developer further customize programs created with the IDE tools.
- The *e-Biz Impact TRAN-IDE Guide* describes how to use the TRAN-IDE tool to build e-Biz Impact production objects, which define incoming data and the output transactions produced from that data.

Note The *e-Biz Impact ODL Application Guide* has been incorporated into the *e-Biz Impact ODL Guide*.

The *e-Biz Impact Alerts Guide*, the *e-Biz Impact SNMP Guide*, and the *e-Biz Impact Global Console Guide* have been combined into a new guide—*Monitoring e-Biz Impact*.

Adaptive Server Anywhere documentation The e-Biz Impact installation includes Adaptive Server® Anywhere, which is used to set up a Data Source Name (DSN) used with e-Biz Impact security and authorization. To reference Adaptive Server Anywhere documentation, go to the Sybase Product Manuals Web site at Product Manuals at http://www.sybase.com/support/manuals/, select SQL Anywhere Studio from the product drop-down list, and click Go.

Note Read the *SyBooks Installation Guide* on the Getting Started CD, or the *README.txt* file on the SyBooks CD for instructions on installing and starting SyBooks.

Other sources of information

Use the Sybase Getting Started CD, the SyBooks CD, and the Sybase Product Manuals Web site to learn more about your product:

- The Getting Started CD contains release bulletins and installation guides in PDF format, and may also contain other documents or updated information not included on the SyBooks CD. It is included with your software. To read or print documents on the Getting Started CD, you need Adobe Acrobat Reader, which you can download at no charge from the Adobe Web site using a link provided on the CD.
- The SyBooks CD contains product manuals and is included with your software. The Eclipse-based SyBooks browser allows you to access the manuals in an easy-to-use, HTML-based format.

  Some documentation may be provided in PDF format, which you can access through the PDF directory on the SyBooks CD. To read or print the PDF files, you need Adobe Acrobat Reader.

  Refer to the *SyBooks Installation Guide* on the Getting Started CD, or the *README.txt* file on the SyBooks CD for instructions on installing and starting SyBooks.
- The Sybase Product Manuals Web site is an online version of the SyBooks CD that you can access using a standard Web browser. In addition to product manuals, you will find links to EBFs/Maintenance, Technical Documents, Case Management, Solved Cases, newsgroups, and the Sybase Developer Network.

  To access the Sybase Product Manuals Web site, go to Product Manuals at http://www.sybase.com/support/manuals/.

Sybase certifications on the Web

Technical documentation at the Sybase Web site is updated frequently.

❖ **Finding the latest information on product certifications**

1. Point your Web browser to Technical Documents at http://www.sybase.com/support/techdocs/.
2. Select Products from the navigation bar on the left.
3. Select a product name from the product list and click Go.
4. Select the Certification Report filter, specify a time frame, and click Go.
5. Click a Certification Report title to display the report.

❖ **Creating a personalized view of the Sybase Web site (including support pages)**

Set up a MySybase profile. MySybase is a free service that allows you to create a personalized view of Sybase Web pages.

1 Point your Web browser to Technical Documents at http://www.sybase.com/support/techdocs/.

2 Click MySybase and create a MySybase profile.

Sybase EBFs and software maintenance

❖ **Finding the latest information on EBFs and software maintenance**

1 Point your Web browser to the Sybase Support Page at http://www.sybase.com/support.

2 Select EBFs/Maintenance. Enter user name and password information, if prompted (for existing Web accounts) or create a new account (a free service).

3 Select a product.

4 Specify a time frame and click Go.

5 Click the Info icon to display the EBF/Maintenance report, or click the product description to download the software.

Conventions

The syntax conventions used in this manual are:

Key	Definition
commands and methods	Command names, command option names, utility names, utility flags, Java methods/classes/packages, and other keywords are in lowercase Arial font.
variable	Italic font indicates: • Program variables, such as *myServer* • Parts of input text that must be substituted, for example: *Server*.log • File names
File | Save	Menu names and menu items are displayed in plain text. The vertical bar shows you how to navigate menu selections. For example, File | Save indicates "select Save from the File menu."

Key	Definition
`package 1`	Monospace font indicates: • Information that you enter in a graphical user interface, at a command line, or as program text • Sample program fragments • Sample output fragments

Accessibility features

This document is available in an HTML version that is specialized for accessibility. You can navigate the HTML with an adaptive technology such as a screen reader, or view it with a screen enlarger.

For information about how Sybase supports accessibility, see Sybase Accessibility at http://www.sybase.com/accessibility. The Sybase Accessibility site includes links to information on Section 508 and W3C standards.

If you need help

Each Sybase installation that has purchased a support contract has one or more designated people who are authorized to contact Sybase Technical Support. If you cannot resolve a problem using the manuals or online help, please have the designated person contact Sybase Technical Support or the Sybase subsidiary in your area.

CHAPTER 1

Overview

This chapter presents an overview of e-Biz Impact security using role-based authorization.

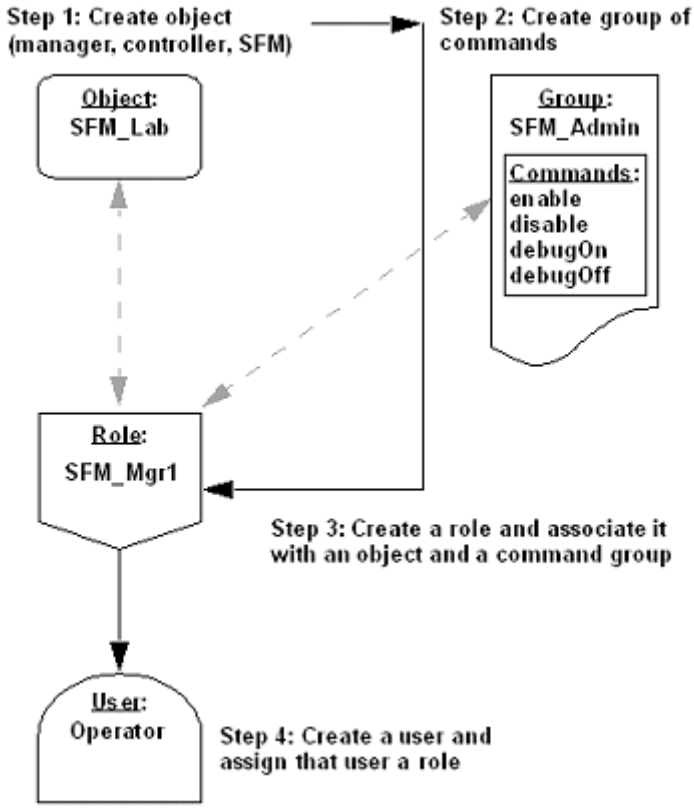
Introduction

e-Biz Impact security allows you to define role-based authorization for command and control (CNC) requests that are executed using the Global Console, the CNC command line utility, and the Java remote.CncProxy.

To implement e-Biz Impact security, you set up Data Source Names (DSNs) that represent ODBC database connections for the Authorization Console and each cluster in your environment. These connections allow the authorization client (Authorization Console) and the e-Biz Impact server-hosted cluster to communicate with the authorization database.

Once you have created the DSNs, you use the Authorization Console to define roles that you associate with objects and groups. This builds a security policy that authorizes a role to execute commands defined in the group against the selected object. When you create a user and assign that user a role, they are authorized to execute the commands on the object associated with that role.

Figure 1-1: Setting up security in the Authorization Console



For example, Figure 1-1 illustrates how you can create the SFM_Lab object, then associate that object with the SFM Administration group of commands. You create the SFM_Mgr1 role, then assign the Operator user that role. Because the Operator user has the SFM_Mgr1 role, they are authorized to perform the SFM Administration commands on the SFM_Lab1 object.

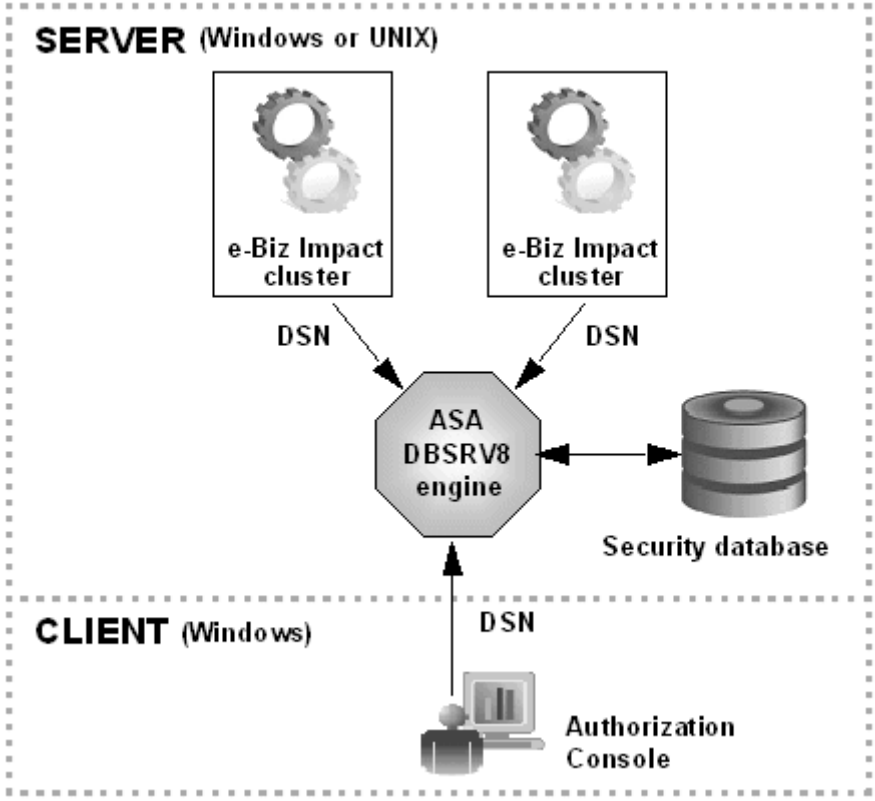
If you choose not to use e-Biz Impact security:

- You do not have to run the authorization database to use the Global Console.
- All users can execute all commands from the Global Console, from the CNC command line utility, and with the Java remote.CncProxy.

Implementation

Security roles are stored in a Adaptive Server Anywhere database, which is installed with the e-Biz Impact server. Before you create security objects, groups, roles, and users, you must create the DSN connections that allow the Authorization Console and e-Biz Impact server to access the database.

Figure 1-2: Authorization process flow



To use e-Biz Impact role-based authorization:

1 Install e-Biz Impact. The Adaptive Server Anywhere software is installed with e-Biz Impact server. See the e-Biz Impact installation guide.

2 Set up an authorization database for each cluster you have defined in your e-Biz Impact environment, or use the authorization database impact.db that is installed with e-Biz Impact.

Note Do not use the *impact.db* template file as is; rather, create a copy and modify the file for your own needs. Use only one copy of the database per directory. Multiple copies of the database in the same directory cause conflicts at runtime.

3 Use the instructions in Chapter 2, "Configuring Security Database Connections," to:

   a Create a client Data Source Name (DSN) on the Windows machine where the Authorization Console is installed.

   b Create a server DSN for each cluster in your e-Biz Impact implementation.

4 Use the instructions in Chapter 3, "Setting Up Role-Based Authorization,"to start authorization database, start the Authorization Console, log in to the authorization database, and create the security entities and role assignments that implement your enterprise's security protocols.

5 Use the instructions in the *e-Biz Impact Configurator Guide*, Chapter 2, "Configuring Clusters" to enable authorization for yours clusters. To use e-Biz Impact's authorization capabilities, you must select the Security option on the Cluster Properties Advanced tab in the Configurator. If the Security option is not selected, a cluster ignores the security settings specified in the Authorization Console. See for instructions.

CHAPTER 2

Configuring Security Database Connections

This chapter describes how to configure the database connections required to implement e-Biz Impact security.

Introduction

Before you set up role-based security in the Authorization Console, you must establish a system Data Source Name (DSN) to provide connectivity to the authorization database through an ODBC driver.

You need two DSNs—one DSN for the Authorization Console client, and one DSN that allows the e-Biz Impact server to connect to the authorization database, which lets you execute command and control (CNC) requests on cluster objects from the Global Console, the command line utility, or the Java remote.CncProxy

Note When you complete the procedures in this chapter, proceed to Chapter 3, “Setting Up Role-Based Authorization,” to finish configuring e-Biz Impact security.

Creating the cluster security database DSN

This section describes how to create the DSN that provides connectivity from e-Biz Impact server clusters to the authorization database.

You must create a DSN for each cluster in your e-Biz Impact implementation, and create the DSN on the system where the e-Biz Impact server and authorization database are installed.

If the e-Biz Impact server is installed on Windows, go to "Creating the cluster DSN on Windows" on page 7.

If the e-Biz Impact server is installed on a UNIX system, go to "Creating the cluster DSN on UNIX" on page 6.

Creating the cluster DSN on UNIX

Use this procedure if the e-Biz Impact server is installed on a UNIX system.

❖ **Creating the cluster DSN on UNIX**

1 Navigate to the *odbc.ini* file, which is located in:

../Sybase/ImpactServer-5_4/odbc

2 Open *odbc.ini* in a text editor.

3 Add a DSN entry to [ODBC Data Sources] stanza.

In the [ODBC Data Sources] section; after the line "ASA=Adaptive Server Anywhere," add:

```
IMPACT_DSN=Adaptive Server Anywhere
```

where *IMPACT_DSN* must match the Data Source Name that you specify for the DSN for the Authorization Console client; for example, `Auth_DSN`.

4 Add the DSN connectivity information to the end of the file. At the end of the file, add these lines:

```
[IMPACT_DSN]
Driver=/Sybase/ImpactServer-5_4/asa/libdbodbc8_r.so
Description=Adaptive Server Anywhere
CommLinks=tcpip(DOBROADCAST=DIRECT;HOST=localhost;PORT=2638)
ServerName=IMPACT
```

where the Driver path, PORT number, and ServerName should reflect your environment, and must correspond to the values used to start the authorization database. If necessary, change the library extension (***.so***) according to the UNIX platform on which you are creating the DSN.

5 Save the file and close the text editor.

Creating the cluster DSN on Windows

Use this procedure if the e-Biz Impact server is installed on a Windows system.

❖ **Creating the cluster DSN on Windows**

1 On Windows, select Start | Settings | Control Panel.

2 Select Administrative Tools | Data Sources (ODBC). The ODBC Data Source Administrator window appears.

3 Select the System DSN tab and click Add.

4 From the driver list, select "Ims54 Adaptive Server Anywhere 8" and click Finish.

Note If you have the server and client installed on Windows, two entries display in the driver list ("`Imc54..`" for the client and "`Ims54..`" for the server). *Select the server entry for this procedure.*

---

5 When the ODBC Configuration for Adaptive Server Anywhere 8 window appears, complete these options on the ODBC tab:

- Data Source Name – tells the ODBC driver manager or Embedded SQL™ library where to look in the file or registry to find ODBC data source information.

  Enter any unique descriptive name for the cluster DSN (spaces are allowed); for example, `Cluster1_dsn`. Keep the name short; you may need to enter it in connection strings.

- Description – enter an optional longer description of the data source to help you or end users to identify this data source from among their list of available data sources.

6 Select the Login tab, then select Supply User ID and Password, but leave the actual user ID and password fields blank.

7 Select the Database tab. This tab's options let you specify the authorization database to use, and whether to start the database automatically.

- Server Name – the name of the local Adaptive Server Anywhere (`dbsrv8`) or the network database server where the security information is stored.

- Start Line – enter this value only if you want the authorization database to start automatically when you try to execute a cluster command from the Global Console, from the command line utility, or from Java remote.CncProxy.

  For example:

  ```
  x:\Sybase\ImpactServer-5_4\asa\dbsrv8.exe
  ```

  where "*x*" is the drive on which the e-Biz Impact 5.4 Server is installed. If you want to start the authorization database manually, leave this field blank.

  Note To start the authorization database automatically, you must provide a Start Line and select the option "Automatically start the database if it isn't running."

- Database Name – enter the name of the Adaptive Server Anywhere database to which you want to connect—`impact`.

  Warning! Do not enter *impact.db* for the database name.

- Database file – enter the full path and name of the Adaptive Server Anywhere database file. Click Browse to locate the file. For example:

  ```
  D:\Sybase\ImpactServer-5_4\bin\impact.db
  ```

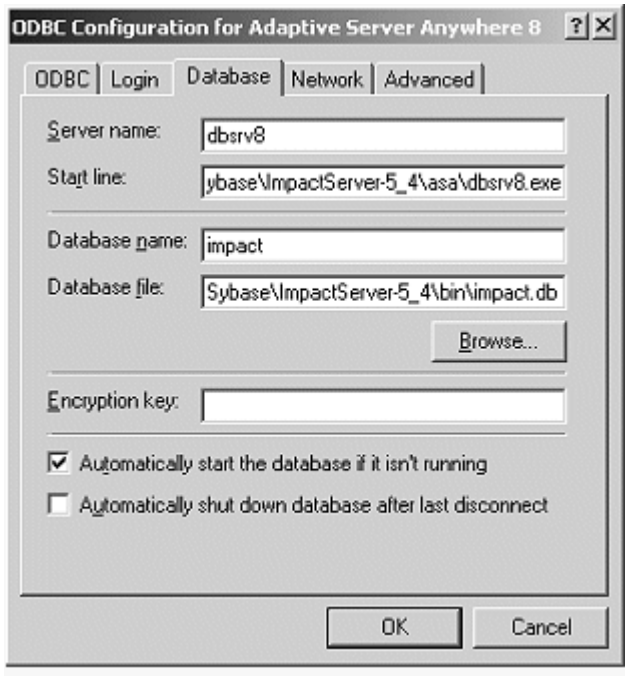
- Encryption Key – leave this field blank.
- Automatically start the database if it isn't running – select this option to start the authorization database automatically when you execute a cluster command from the Global Console, from the command line utility, or from Java remote.CncProxy.

  Warning! When this option is selected, you must also have a Start Line entry.

- Automatically shut down database after last disconnect – leave this option unselected to leave the authorization database running once it is started.

When you finish, and have chosen to automatically start the authorization database, the Database tab entries should look similar to the screen shown in Figure 2-1

Figure 2-1: Cluster ODBC DSN Database tab entries



If you chose to start the authorization database manually, the Start Line will be empty and the "Automatically start." option is unselected.

8 Select the Network tab and verify that the only options selected are Shared Memory and None (for encryption of network packages). The TCP/IP option should not be selected.

Accept the default values for the time-outs and buffer size.

❖ **Testing the cluster DSN with an automatic database connection**

1 If you chose to start the authorization database automatically, select the ODBC tab in the ODBC Configuration window and click Test Connection. You should see this message:

```
Connection Failed: Integrated logins are not
permitted.
```

Although the message indicates that the connection failed, the message actually means that the DSN configuration is successful.

Note If you receive the following message, verify your parameters, particularly, host, port, and server name:

```
Connection Failed: Database server not found.
```

2 Click OK to save your entries and close the ODBC Configuration window.

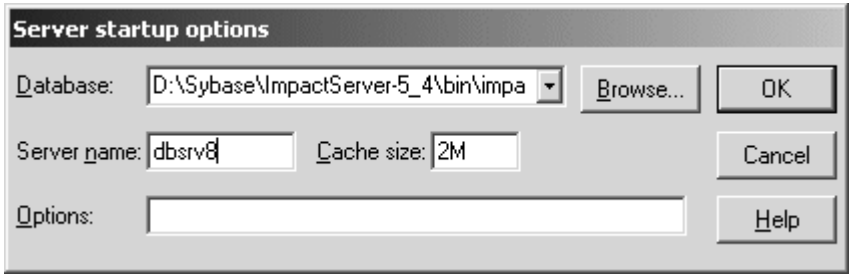
3 Click OK to save the DSN and exit the ODBC Data Source Administrator.

❖ **Testing the cluster DSN with a manual database connection**

If you chose not to start the authorization database automatically, you must start the database manually to test the connection.

1 Go to *x:\Sybase\ImpactServer-5_4\asa* (where "*x*" is the drive or directory where the e-Biz Impact server is installed) and double-click *dbsrv8.exe* to start Adaptive Server Anywhere.

The Server Start-up Options dialog box appears.



2 Complete these options:

- Database – use the Browse button to navigate to and select the authorization database. For example, if you are using the Sybase-provided database *impact.db*, this entry could be:

  `x:\Sybase\ImpactServer-5_4\bin\impact.db`

  where "*x*" is the directory or drive on which the e-Biz Impact server is installed.

- Server Name – enter `dbsrv8`.

Leave the remaining options as they are and click OK. An Adaptive Server Anywhere status window appears and states that you have successfully connected to the database. When the last line displays, "Now accepting requests," the window automatically minimizes.

3 In the ODBC Configuration window, select the ODBC tab and click Test Connection. You should see this message:

```
Connection Failed: Integrated logins are not
permitted.
```

Although the message indicates that the connection failed, the message actually means that the DSN configuration is successful.

Note If you receive the following message, verify your parameters, particularly, host, port, and server name:

```
Connection Failed: Database server not found.
```

4 Click OK to save your entries and close the ODBC Configuration window.

5 Click OK to save the DSN and exit the ODBC Data Source Administrator.

6 To shut down the authorization database, right-click the dbsrv8 icon that appears on the far right of the task bar and select Exit.

Creating the Authorization Console security database DSN

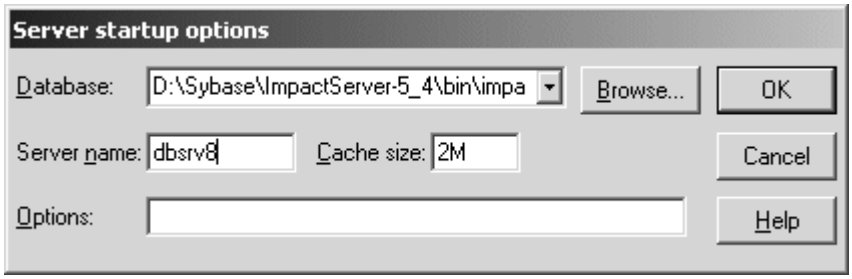
This section explains how to create a DSN for the Authorization Console.

Note Because the Authorization Console only runs on Windows, you need to perform this procedure only on the Windows machine where the Authorization Console is installed.

❖ **Creating the Authorization Console DSN**

1 Go to *x:\Sybase\ImpactServer-5_4\asa* (where "*x*" is the drive or directory where the e-Biz Impact server is installed) and double-click *dbsrv8.exe* to start Adaptive Server Anywhere.

The Server Start-up Options dialog box appears.



2 Complete these options:

- Database – enter the path to the database (for example, *x:\Sybase\ImpactServer-5_4\bin\impact.db*, where "*x*" is the drive where the e-Biz Impact security database is located) or Browse to locate the authorization database.
- Server Name – enter `dbsrv8`.

Leave the remaining options as they are and click OK. An Adaptive Server Anywhere status window appears and states that you have successfully connected to the database. When the last line displays, "Now accepting requests," the window automatically minimizes.

3 On Windows, select Start | Settings | Control Panel.

4 Select Administrative Tools | Data Sources (ODBC). The ODBC Data Source Administrator window appears.

5 Select the System DSN tab and click Add.

6 From the driver list, select "`Imc54 Adaptive Server Anywhere 8`" and click Finish.

Note Typically, you install the e-Biz Impact server on a UNIX machine and install the e-Biz Impact client on a Windows machine. If you have the server and client installed on Windows, two entries display in the driver list ("Imc54.." for the client and "Ims54.." for the server). *Select the client entry for this procedure.*

---

7 When the ODBC Configuration for Adaptive Server Anywhere 8 window appears, complete these options on the ODBC tab:

- Data Source Name – tells the ODBC driver manager or Embedded SQL™ library where to look in the file or registry to find ODBC data source information.

  Enter any unique descriptive name for the authorization DSN (spaces are allowed); for example, `Auth_DSN`. Keep the name short; you may need to enter it in connection strings.

- Description – enter an optional longer description of the data source to help you or end users to identify this data source from among their list of available data sources.

8 Select the Login tab, then select Supply User ID and Password, but leave the actual user ID and password fields blank.

9 Select the Database tab and complete these options:

- Server Name – the name of the local Adaptive Server Anywhere (`dbsrv8`) or the network database server where the security information is stored.
- Start Line – leave this field empty.
- Database Name – enter the name of the Adaptive Server Anywhere database to which you want to connect—`impact`.

  Warning! Do not enter *impact.db* for the database name.

- Database file – leave this field blank.
- Encryption Key – leave this field blank.
- Automatically start the database if it isn't running – leave this option unselected.
- Automatically shut down database after last disconnect – leave this option unselected.

  When you finish, the Database tab entries should look similar to the screen shown in Figure 2-2

Figure 2-2: Authorization Console ODBC DSN Database tab entries

Only the Server Name and Database Name should be filled in.

10 Select the Network tab and verify that the only options selected are Shared Memory and None (for encryption of network packages). The TCP/IP option should not be selected.

Accept the default values for the time-outs and buffer size.

❖ **Testing the Authorization Console DSN**

1 Select the ODBC tab and click Test Connection. You should see this message:

```
Connection Failed: Integrated logins are not
permitted.
```

Even though the message indicates that the connection failed, the message actually means that the DSN configuration is successful.

Note If you receive the following message, verify your parameters, particularly, host, port, and server name:

```
Connection Failed: Database server not found.
```

2 Click OK to save your entries and close the ODBC Configuration window.

3 Click OK to save the DSN and exit the ODBC Data Source Administrator.

4 To shut down the authorization database, right-click the dbsrv8 icon that appears on the far right of the task bar and select Exit.

Note Proceed to Chapter 3, “Setting Up Role-Based Authorization,” to finish configuring e-Biz Impact security.

CHAPTER 3

Setting Up Role-Based Authorization

This chapter describes how to use the Authorization Console to create the objects, roles, groups, and users to implement role-based authorization in e-Biz Impact.

Introduction

The e-Biz Impact Authorization Console, allows you implement role-based security that authorizes users to execute commands against cluster objects. Security roles are stored in Sybase Adaptive Server Anywhere database tables and used to verify permissions and roles for e-Biz Impact operations.

Note Adaptive Server Anywhere is installed as part of the e-Biz Impact product installation. You must set up the database connections to the authorization database before you can use the Authorization Console. If you have not done this already, complete the procedures in Chapter 2, “Configuring Security Database Connections.”

Requirements

When you use the Authorization Console to configure role-based authorization, note the following:

- Multiple clusters can share a single authorization database, but the object names must be unique.
- When you modify security entities using the Authorization Console, the modifications are immediately available to clusters that use the associated authorization database; that is, the authorization database to which you are connected in the Authorization Console.
- All command and control (CNC) requests are authorized by the e-Biz Impact server.
- e-Biz Impact version 5.4.2 and later limit the scope of commands to only cluster-defined objects.
- Object names must be unique within any authorization database.
- Clusters that use security must have all clusters (managers), controllers, and SFM objects defined in the Configurator and represented in the authorization database.
- A role assigned to the Manager Administration, Controller Administration, or SFM Administration group can only authorize users if the objects against which they are executed are defined in the security database.
- A role assigned to a Manager object and the Manager Administration group authorizes execution of all commands against a cluster, any children controllers, and SFMs.
- A role assigned to a Controller object and the Controller Administration group authorizes execution of all commands against a cluster's controllers and any children SFMs.
- A role assigned to an SFM object and the SFM Administration group authorizes execution of all commands against a cluster's SFM.

Executing common tasks

- To control objects in multiple clusters, define a role for each Manager object, and assign the role the Manager Administration group.

- To control cluster state, define a role for a Manager object and assign the role a group containing cluster commands (shutdown, reload, and so on).
- To manage the state of a controller, define a role that uses the controller's parent cluster, and assign the role a group containing controller commands (enable, disable, and so on).
- To control standard application state such as ODL (including SFM objects), Java, C/C++, and WebSphere MQ, define a role that uses the application's parent controller, and assign the role a group containing controller commands (enable, disable, and so on).
- To control destinations, define a role that uses the destination's parent SFM, and assign the role a group containing SFM commands (resumeDest, pauseDest, pauseAllDest, resumeAllDest, and so on).
- To control SFM transaction flow, define a role for an SFM object, and assign the role a group containing SFM commands (refuse, accept, and so on).
- Assign a role to a user that authorizes the permissions defined by the role, based on the role's assigned object and group.

Executing complex tasks

Complex actions, such as resubmitting a transaction to a specific destination, usually include one or more command line requests. To ensure that an individual can execute all of the commands associated with a task, you must add the user to a role that is associated with a group that includes authorization to execute all of the task's commands.

Table 3-1 lists the commands you must add to a group to ensure execution of the associated task.

Table 3-1: Complex tasks and associated command

To authorize this task	Add these commands to a group
Resend a transaction to all destinations for which the transaction qualifies	pauseDestsBySerial resendTransactionBySerial resumeDestsBySerial
Resend a transaction to a specific destination	pauseDest resendTransactionBySerial resumeDest

To authorize this task	Add these commands to a group
Skip transactions for all destinations for which the transaction qualifies	pauseDestsBySerial skipTransactionBySerial resumeDestsBySerial
Skip a transaction for a specific destination	pauseDest skipTransactionBySerial resumeDest
Cancel a transaction for all destinations for which the transaction qualifies	pauseDestsBySerial cancelTransactionBySerial resumeDestsBySerial
Cancel a transaction for a specific destination	pauseDest cancelTransactionBySerial resumeDest
Uncancel and repair cancelled transactions: access the cancelled transactions SFM view	getTransactionList
Uncancel and repair cancelled transactions: repair a cancelled transaction	pauseDestsBySerial resubmitTransaction resumeDestsBySerial
Uncancel a transaction for all destinations for which the transaction qualifies	pauseDestsBySerial uncancelTransactionBySerial resumeDestsBySerial
Uncancel a transaction for a specific destination	pauseDest uncancelTransactionBySerial resumeDest
Unprocessable transactions: access the unprocessable transactions SFM view	getTransactionList
Unprocessable transactions: skip an unprocessable transaction	pauseDestsBySerial skipUnprocessableTransaction resumeDestsBySerial
Unprocessable transactions: cancel an unprocessable transaction	pauseDestsBySerial cancelUnprocessableTransaction resumeDestsBySerial
Unprocessable transactions: resubmit an unprocessable transaction	getTransactionData resubmitTransaction
Unrouteable transactions: access the unrouteable transactions SFM view	getTransactionList

To authorize this task	Add these commands to a group
Unrouteable transactions: delete an unrouteable transaction	deleteUnrouteableTransaction
Unrouteable transactions: resubmit an unrouteable transaction	getTransactionData resubmitTransaction

To add new command authorization to a group, right-click the group in the right pane and select All Tasks | New Command. See "Adding commands to a group" on page 28.

Starting the authorization database

Before you start the Authorization Console to configure e-Biz Impact security, start the authorization database. This section describes how to start the database on both Windows and UNIX systems.

❖ **Starting the authorization database on Windows**

1 Go to *x:\Sybase\ImpactServer-5_4\asa* (where "*x*" is the drive or directory where the e-Biz Impact server is installed) and double-click *dbsrv8.exe* to start Adaptive Server Anywhere.

2 When the Server Start-up Options dialog box opens, complete the options:

- Database – use the Browse button to navigate to and select the authorization database. For example, if you are using the Sybase-provided database *impact.db*, this entry could be:

  `x:\Sybase\ImpactServer-5_4\bin\impact.db`

  where "*x*" is the directory or drive where the e-Biz Impact server is installed.

- Server Name – enter `dbsrv8`.

  Leave the remaining options as they are.

- Click OK.

An Adaptive Server Anywhere status window appears and states that you have successfully connected to the database. When the last line displays, "Now accepting requests," the window automatically minimizes.

❖ **Starting the authorization database on UNIX**

1 Set the following environment variables in a terminal window or add them to your login *.profile*, changing the *ASA_ROOT* value to match the installation of your e-Biz Impact server.

```
ASA_ROOT=[e-Biz Impact install location]/Sybase/ImpactServer-5_4/asa
PATH=$ASA_ROOT/bin:$PATHLIB
PATH=$ASA_ROOT/lib:$LIBPATH
ASANY=$ASA_ROOTODBCINI=$NNSY_ROOT/odbc.ini

export ASA_ROOT PATH LIBPATH ASANY ODBCINI
```

Note The default *ODBCINI* value is shown above. If you change this value, be aware that the ims wrapper script, which is used to start clusters, may be using the default value. If you have applications that require database connectivity, the ims wrapper script overrides any environment variables set in the user's *.profile*. If the application cannot locate the *odbc.ini* file, or is referencing the incorrect one, it will fail to connect or behave unexpectedly. See the e-Biz Impact Configuration Guide, Chapter 5, "Deploying Files and Executing the e-Biz Impact Cluster," for more information about wrapper scripts.

2 Enter this command on one line to launch the authorization database:

```
ims.db dbsrv8 -n [SERVER NAME] -x "tcpip(PORT=NNNN)" [authorization
database].db
```

- `-n` *[SERVER NAME]* – the unique user-defined name given when running the database server process. This name must match:
  - The Server Name entered on the Database tab when you created the ODBC DSN for the client.
  - The ServerName entered for the DSN in the *odbc.ini* file when you created the ODBC DSN for the server.
- `-x "tcpip (PORT=`*NNNN*`)"` – the PORT used to start the server. The default port number is 2638. Replace *NNNN* with the TCP/IP port on which the database accepts connection requests. This port must be unique and unused by other applications on the machine.

Note Because the database server always listens on port 2638, even if you specify a different port using a network communication parameter, applications can connect to the database without specifying a port number.

However, an exception is the HP-UX operating system, on which the server does not listen on port 2638 if it is started on another port.

- *[AUTHORIZATION DATABASE]* – the name of the authorization database, including the absolute path.

Example

For example, if your settings are:

- SERVER NAME = IMPACT_ADT_DB
- PORT = 2638
- Authorization database = impact_adt_db.db
- Database file location = */sybase/clusters/prod/auth*

You would enter this command on one line to launch the authorization database:

```
dbsrv8 -n IMPACT_ADT_DB -x "tcpip(PORT=2638)" /sybase/clusters/prod/auth
     /impact_adt_db.db
```

Starting the Authorization Console

To start the Authorization Console:

1 Select Start | Programs | Sybase | e-Biz Impact 5.4 | Authorization. The Authorization Console appears, with an e-Biz Impact Authorization node beneath the console root.

2 Right-click e-Biz Impact 5.4 Authorization and select New | Connection.

3 When the New Connection dialog box opens, select the client Data Source Name that you previously created for the Authorization Console (for example, Auth_DSN), then click OK.

Logging in to the Authorization database

1 In the console tree pane, right-click the new connection and select All Tasks | Login. You see the Login window.

2 The system populates the Connection name with the new DSN. Enter your Administrator name and password. The default is “admin” and “admin”.

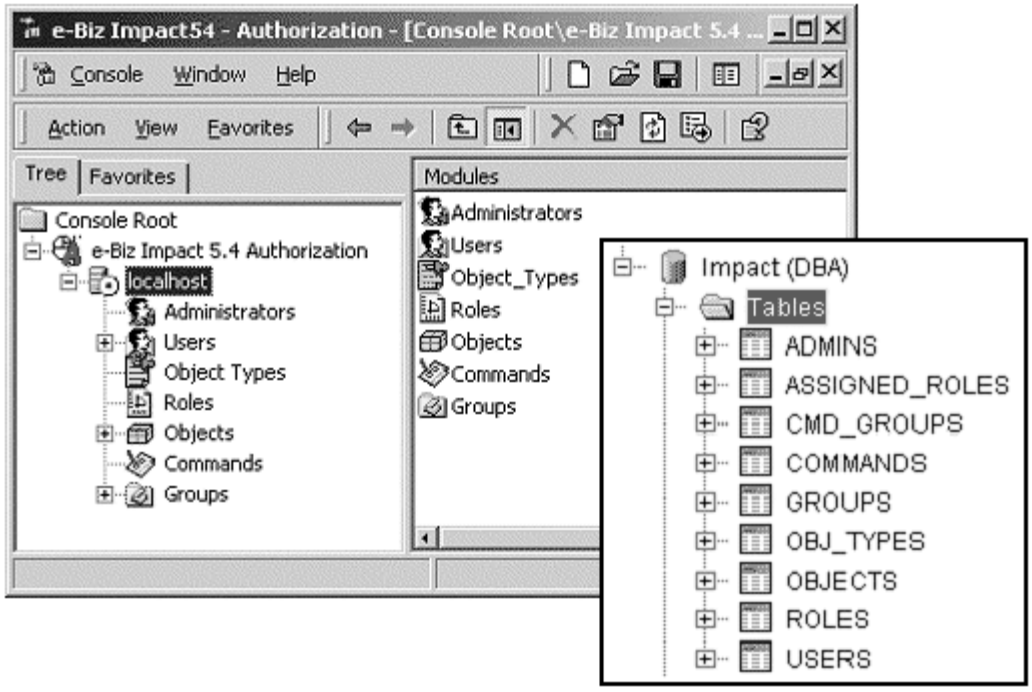
Note Only security administrators can access and configure security policies in the Authorization database.

3 If your organization’s security standards allow you to enable password persistence, select Remember Password and click OK.

Configuring authorization

Once you establish a connection in the Authorization Console, the tree view (left pane) displays modules in use by cluster security—Administrators, Users, Object Types, Roles, Objects, Commands, and Groups. Each module represents a table in the authorization database.

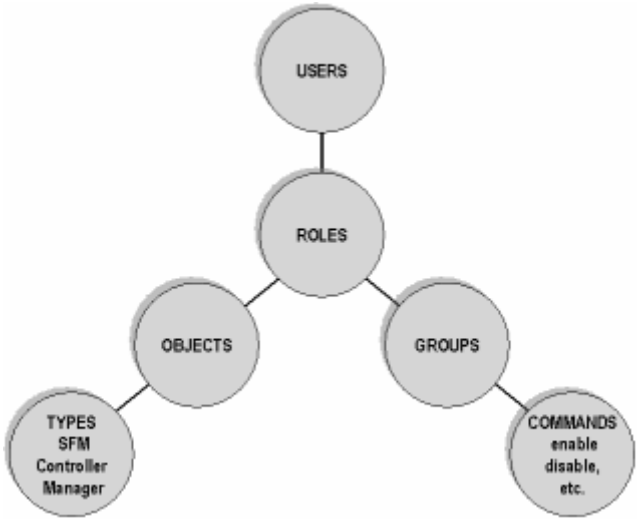
Figure 3-1: Authorization Console



When you select module in the tree view, the right pane displays the individual objects within that module.

The rest of this chapter describes how to configure the authorization components. The relationship of these components to one another is illustrated in Figure 3-2.

Figure 3-2: Authorization architecture



To configure security, follow these steps:

1 Set up the administrator user that creates the security policy for the e-Biz Impact implementation. See “Setting up administrators” on page 26.

2 Define the objects upon which you want to implement security. See “Defining objects” on page 27.

3 Create groups and add commands to the groups. See “Defining groups” on page 28 and “Adding commands to a group” on page 28.

4 Define roles and associate each role with an object and a group. Users that are assigned a role have permission to execute the commands associated with that role’s group and object. See “Defining roles” on page 29.

5 Create users and assign them roles. See “Defining users” on page 29.

Setting up administrators

An e-Biz Impact security administrator creates and assigns roles using the Authorization Console. Initially, only a user with administrative privileges and the user name and password “admin” can create and delete other users (including administrators), and reset administrator passwords. Administrators can monitor all items in a connection tree.

When you set up the DSN, start the Authorization Console, and log in, the default Manager Administrator user has already been set up automatically.

Warning! The e-Biz Impact security administrator should change the default administrator password after installation.

❖ **Adding new administrators**

1 Right-click Administrators in the tree view and select New | Administrator. A default name is assigned. To change the system-assigned name, right-click the name in the detail pane and select Rename. Type the new name and press Enter.

2 Enter a new password, then enter the password again and click OK.

❖ **Modifying administrator properties**

1 Right-click the administrator name in the detail pane.

2 Select a menu option:

- All Tasks | Set Password – to change the selected administrator's password. Enter the New Password, then enter the password again to confirm and click OK.
- Rename – to change this administrator's name. New administrator names are automatically assigned. To change the system-assigned name, type the new name and press Enter.
- Delete – to delete the selected administrator. To confirm that you want to delete the selected administrator, click OK.

Defining objects

Objects are entities that represent the e-Biz Impact infrastructure and the server and cluster structure for which you are defining security.

The Authorization Console allows you to create three object types—managers (clusters), controllers, and SFMs. These are the only available object types, because these are the only objects on which you can execute commands for which you can control authorization.

Use the manager to create controller objects, and use the controller to create SFM objects. Manager and controller objects can issue commands, while only SFM objects can receive CNC commands.

To create a new object, right-click Objects in the tree pane and select New. Name the object, select the associated object type, and click OK.

You can also select a parent object, then use the All Task menu item to create the appropriate object:

- If the parent object is a manager, select New | Controller.
- If the parent object is a controller, select New | SFM.

Each object is given a default name (you can rename the objects) and assigned one of the following types: SFM, controller, or manager. You can also import the object tree from your cluster configuration (the *<cluster-name>.xml* file generated by Configurator).

Note Object names must be unique within any authorization database.

Defining groups

A group manages a user-defined set of commands. The Authorization Console provides three predefined groups—Controller Administration, Manager (Cluster) Administration, and SFM Administration. You cannot add, change, or delete commands for these groups.

For example, you can create a new group that is allowed to shut down and reload the manager. You can define group names by using functional areas such as monitoring, Web modules, or technical areas such as AIM management.

To define a group, select Group | New Group from the tree pane. A new group (default name Group_n) is created and appears in the detail pane. To rename the group and add a description, right-click and select Properties.

Adding commands to a group

A group is made up of commands. Add commands to groups to easily manage e-Biz Impact operations. Object types (controller, cluster, and SFM) are associated with a number of monitoring commands. To view the list of available commands, select Commands in the tree pane. The commands and their associated object types are listed in the detail pane.

To add a command to a group, simply drag the commands and drop them on the group. All commands assigned to a group must be of the same object type.

See “Executing complex tasks” on page 19 for a list of the commands that you must have permission to execute for specific cluster tasks.

Note You cannot modify the commands associated with the predefined e-Biz Impact groups.

Defining roles

A role links a group of commands to the object upon which they can be executed. A role is then assigned to a user, authorizing him to execute any commands within the group.

When defining a role, you are prompted to select an object and group. This builds a security policy that authorizes a role to execute commands defined in the group against the selected object. For example, create a role for SFM1 that allows the SFM Administration group of commands. Assign the newly-created role to the user Operator.

To create a new role, select the object, right-click, and select the appropriate group of commands you want to add. Accept the default name and click Next. Click OK to return to the main window.

To create a role directly from an object, select an object, right-click, and select All Tasks | Create a Role, then select the command group name.

Defining users

A user (Global Console operator) is granted access to the e-Biz Impact Server and assigned roles. This also applies to users specified in the CNC command line tool scripts.

❖ Adding new users and assigning them roles

When you create a new user, you assign them a user name, password, and role.

1 Right-click Users in the tree view and select New | User. A default name is assigned. Enter a different user name or accept the default.

2 Click Password.

3 When the Set Password dialog box opens, enter a New Password, enter the password again to confirm it, then click OK.

4 Click Assign a Role. A role links a group of commands to the object upon which they can be executed. A role is then assigned to a user, authorizing him or her to execute any commands within the group.

5 When the Assign Role dialog box opens, select a role from the drop-down list, then click OK.

You can assign a user one or more roles. When you select a user in the tree view, its associated roles and objects appear in the right pane.

❖ **Modifying user properties**

1 Right-click the user name in the tree view or right pane, then select:

- All Tasks | Set Password to modify the user's password. When the Set Password window displays, enter the new password, re-enter the password for confirmation, then click OK.
- All Tasks | Assign Role to assign a role that authorizes the user to execute commands against objects. When the Assign Role window displays, select the role to assign, then click OK. You can also drag and drop a role to a user node to assign them that role.

Note You can also right-click the user name and select Properties to reset the password or assign a new role.

2 To remove a user from the database, right-click the user name and select Delete.

3 To remove a role from a user, right-click the role in the tree view or right pane, then choose Delete.

Enabling security for clusters

Use the instructions in the *e-Biz Impact Configurator Guide*, Chapter 2, "Configuring Clusters" to enable authorization for yours clusters. To use e-Biz Impact's authorization capabilities, you must select the Security option on the Cluster Properties Advanced tab in the Configurator. If the Security option is not selected, a cluster ignores the security settings specified in the Authorization Console.

Index

S

U