IBM Tivoli Composite Application Manager for SOA
7.2 Fix Pack 1 (updated November 2015)

Installation Guide

IBM

GC23-8803-05

IBM Tivoli Composite Application Manager for SOA
7.2 Fix Pack 1 (updated November 2015)

Installation Guide

GC23-8803-05

Note

Before using this information and the product it supports, read the information in “Notices” on page 529.

Edition Notice

This edition applies to version 7.2 of IBM Tivoli Composite Application Manager for SOA and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication ix

What this publication contains ix
Intended audience xi
Publications xi
ITCAM for Applications library xi
Related publications xii
Accessing terminology online xiii
Accessing publications online xiii
Ordering publications. xiii
Accessibility xiv
Application Performance Management community on Service Management Connect xiv
Tivoli technical training xiv
Tivoli user groups xiv
Support information xiv
Conventions used in this publication xv
Typeface conventions xv
Operating system-dependent variables and paths xv
Resolving directory path variables xvi

Part 1. Installing the product 1

Chapter 1. Planning an installation . .. 3

Overview 3
IBM Tivoli Monitoring 4
Monitoring agents 5
ITCAM for SOA-specific Data Collectors 6
Data Collectors shared with other products . .. 6
Data Collector for WebSphere Message Broker .. 7
ITCAM Data Collector for WebSphere 7
Application support files 10
SOA Domain Management Server 11
Tivoli Common Object Repository 11
ITCAM for SOA tools 12
Discovery Library Adapters 12
Databases 13
Software and hardware prerequisites 15
Required software 15
Required hardware 16
Considerations for data collectors 17
Performing a pristine installation of ITCAM for SOA version 7.2 Fix Pack 1 19
Before installing ITCAM for SOA 19
Installing Tivoli Monitoring 20
Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1. 20
Upgrading to ITCAM for SOA version 7.2 23
Before upgrading ITCAM for SOA 24
Roadmap for upgrading from ITCAM for SOA version 7.1.1 to version 7.2 26
After upgrading ITCAM for SOA 27
Updating to ITCAM for SOA version 7.2.0.1 . .. 28
Before updating to ITCAM for SOA version 7.2 Fix Pack 1 29
Roadmap for updating from ITCAM for SOA version 7.2 to version 7.2.0.1 30

Chapter 2. Installing or upgrading ITCAM for SOA on Windows systems . 35

Permissions for installing, upgrading, or updating the monitoring agent 35
Installing ITCAM for SOA on a 64-bit system . .. 35
Enabling application support on the monitoring server, portal server, and desktop client 36
Enabling application support through self-description 36
Installing and enabling application support manually before installing the agent 37
Verifying User Account Control settings on Windows 7 platform 39
Installing and upgrading the ITCAM for SOA monitoring agent and data collectors 40
Step 1: Start setup.exe 42
Step 2: Accept the software license agreement .. 42
Step 3: Choose the destination folder for the installation files 42
Step 4: Enter the IBM Tivoli Monitoring encryption key 43
Step 5: Select the product components you want to install 44
Step 6: View the option to remotely deploy monitoring agent 46
Step 7: Select a Windows program folder . .. 47
Step 8: Verify selected features 48
Step 9: Select the items to configure 49
Step 10: Specify the host name of the portal server 51
Step 11: Activate application support if IBM Tivoli Monitoring is installed 51
Step 12: Add the default managed system list when you process application-support files. .. 52
Step 13: View results of application support seeding process 52
Step 14: Finalize the installation or upgrade .. 53
Step 15: Additional procedures in a pristine installation, upgrade, or update. 53
Step 16: Choose a runtime environment to configure for data collection 53
Step 17: Confirm the installation of the ITCAM Data Collector for WebSphere 55
Step 18: Install ITCAM Data Collector for WebSphere 55
Step 19: Configure the ITCAM Data Collector for WebSphere 56
Step 20: Completing the installation and configuration of the data collector 57
Step 21: Verifying the installation of the monitoring agent 58

Step 22: Preparing the Tivoli Enterprise Portal browser client 58
Configuring the monitoring agent 58
Silent installation on Windows systems 61
Preparing response files on Windows systems .. 61
Running the silent installation from a command prompt with parameters 62
Running the silent installation with SMS . .. 63
Configuring for remote deployment of the monitoring agent 63
Adding the installation bundles to the deployment depot 64
Installing the ITCAM for SOA monitoring agent remotely with Tivoli Enterprise Portal 64
Installing the ITCAM for SOA monitoring agent remotely from a command prompt 65
Installing and configuring ITCAM Data Collector for WebSphere from a command prompt . .. 66
Upgrading a remotely deployed ITCAM for SOA monitoring agent 69
Migrating to ITCAM Data Collector for WebSphere from a command prompt 69
Enabling the ITCAM for SOA data collectors on the remote system 72
Uninstalling IBM Tivoli Composite Application Manager for SOA on Windows systems 72
Before uninstalling the monitoring agent . .. 73
Uninstalling the monitoring agent on Windows systems. 73
Installing and uninstalling language support . .. 75
Installing a language pack on Windows systems 75
Uninstalling language packs 75

Chapter 3. Installing ITCAM for SOA on Linux and UNIX systems 77

Enabling application support on the monitoring server, portal server, and desktop client 77
Enabling application support through self-description 77
Installing and enabling application support manually before installing the agent 78
Installing, upgrading, and updating the monitoring agents and data collectors 81
Permissions for installing, upgrading, or updating the monitoring agent 83
Before installing or upgrading the monitoring agent 84
Installing, upgrading, or updating the monitoring agent 84
Configuring the monitoring agent 93
Changing the file permissions for agents . .. 94
Silent installation on Linux and UNIX systems .. 95
Installing the ITCAM for SOA Agent with a response file 96
Performing a silent uninstallation 97
Configuring for remote deployment of the monitoring agent 97
Adding the installation bundles to the deployment depot 98
Installing the monitoring agent remotely with Tivoli Enterprise Portal 98
Installing the monitoring agent remotely from a command line 99
Installing and configuring ITCAM Data Collector for WebSphere from a command line . 100
Upgrading a remotely deployed monitoring agent 102
Migrating to the ITCAM Data Collector for WebSphere from a command-line. 103
Enabling the ITCAM for SOA data collectors on the remote system 106
Uninstalling IBM Tivoli Composite Application Manager for SOA on Linux or UNIX systems. .. 106
Before uninstalling the monitoring agent . .. 106
Uninstalling the monitoring agent on Linux or UNIX systems 107
Installing and uninstalling language support . .. 108
Installing a language pack on UNIX or Linux systems 108
Uninstalling a language pack on UNIX or Linux 109

Chapter 4. Configuring topology support on Windows systems 111

Topology Views and Configuration Options . .. 112
Planning topology support on Windows system 114
Minimum space requirements on the file system 114
Database and User Permissions 115
Creating the SOA Domain Management Server database 120
Manually creating a local SOA Domain Management Server database 121
Manually creating a remote SOA Domain Management Server database 124
Creating the Tivoli Common Object Repository database 127
Manually creating a local Tivoli Common Object Repository database 128
Manually creating a remote Tivoli Common Object Repository database 130
Running the ConfigDMS utility 132
Upgrading from a previous version 133
Launching the `ConfigDMS` utility 135
Running the `ConfigDMS` utility in Graphical User Interface mode 138
Running the `ConfigDMS` utility in console mode 163
Running the `ConfigDMS` utility in silent mode 164
Increasing the report request limit on the portal server 172
Reconfiguring and restarting the Tivoli Enterprise Portal Server 173

Chapter 5. Configuring topology support on Linux systems 175

Topology Views and Configuration Options . .. 176
Planning topology support on Linux or UNIX .. 178
Minimum space requirements on the file system 178
Database and User Permissions 178
Creating the SOA Domain Management Server database 184
Manually creating a local SOA Domain Management Server database 184

Manually creating a remote SOA Domain Management Server database 187
Creating the Tivoli Common Object Repository database 189
Manually creating a local Tivoli Common Object Repository database 189
Manually creating a remote Tivoli Common Object Repository database 192
Running the `ConfigDMS` utility 194
Upgrading from a previous version 195
Launching the `ConfigDMS` utility 197
Running the `ConfigDMS` utility in Graphical User Interface mode 200
Running the `ConfigDMS` utility in console mode 218
Running the `ConfigDMS` utility in silent mode 219
Increasing the report request limit on the portal server 226
Rebuilding and restarting the Tivoli Enterprise Portal Server 227

Chapter 6. Installing the ITCAM for SOA SDMS agent. 229

Installing and configuring the ITCAM for SOA SDMS agent on Windows systems 229
Permissions for installing the ITCAM for SOA SDMS monitoring agent 229
Enabling application support on the monitoring server, portal server, and portal client 230
Installing and Configuring the ITCAM for SOA SDMS agent on Windows 232
Silent installation on Windows systems. 235
Uninstalling the monitoring agent on Windows systems 237
Installing and uninstalling language support 238
Installing and configuring ITCAM for SOA SDMS agent on Linux and UNIX systems 238
Permissions for installing the ITCAM for SOA SDMS monitoring agent 239
Enabling application support on the monitoring server, portal server, and desktop client . .. 239
Installing the ITCAM for SOA SDMS agent on Linux or UNIX systems 242
Silent installation on Linux and UNIX systems 247
Uninstalling the monitoring agent on Linux and UNIX systems 250
Installing and uninstalling language support 250
Configuring for remote deployment of the ITCAM for SOA SDMS agent 251
Adding installation bundles to the deployment depot 251
Installing the ITCAM for SOA SDMS agent remotely with Tivoli Enterprise Portal 253
Installing the ITCAM for SOA SDMS agent remotely from a command prompt 253

Part 2. Configuring a data collector for WebSphere Application Server environments . 255

Chapter 7. Configuring data collection: WebSphere Application Server 257

About the Service Component Architecture . .. 257
Business Process Monitoring 258
Common ITCAM Data Collector for WebSphere 260
Configuring the data collector 260
Installing ITCAM for SOA 7.2, updating to 7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere 261
Installing the data collector when neither the same version nor an older version is configured. 263
Installing the data collector when an earlier maintenance level or an older version is configured 264
Upgrading to V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere 266
Migrating to ITCAM Data Collector for WebSphere when neither the same version nor an older version is configured by another product 268
Migrating to ITCAM Data Collector for WebSphere when an earlier maintenance level or another older version is configured 269
Removing ITCAM for SOA version 7.1.1 WebSphere Application Server data collector .. 271
Updating to V7.2 Fix Pack 1 and configuring ITCAM Data Collector for WebSphere 272
Communicating with ITCAM for Transactions .. 272
Permissions needed to configure data collection 273
Configuring the data collector interactively . .. 273
Configuring ITCAM Data Collector for WebSphere 274
Unconfiguring ITCAM Data Collector for WebSphere 282
Reconfiguring ITCAM Data Collector for WebSphere 284
Migrating data collectors to ITCAM Data Collector for WebSphere. 291
Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere 294
Configuring the data collector is silent mode . .. 298
Configuring ITCAM Data Collector for WebSphere in silent mode 298
Unconfiguring ITCAM Data Collector for WebSphere in silent mode 305
Migrating ITCAM Data Collector for WebSphere in silent mode 308
Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode 312
Limitations when monitoring SCA messages . .. 317
Removing duplicate WebSphere Application Server nodes 317
Logging and Filtering 319
Configuring linking to the BPC Explorer 319

Chapter 8. Advanced configuration and customization of the ITCAM Data Collector for WebSphere 321
Properties files for the Data Collector 321
WebSphere Global Security: setting the user name and password in client properties files 323
Enabling user ID and password input from the sas.client.props file for RMI connector types .. 323
Enabling user ID and password input from the soap.client.props file for SOAP connector types . 324
Configuring the data collector when changing the application server version 324
Configuring data collection for ITCAM for SOA when upgrading IBM BPM 325
Steps to complete if the IP address of the application server host is to be changed 325
What to do when deleting an application server profile 326
Using the root ID for the data collector installation when the application server is not owned and operated by the root ID 326
Increasing the heap size 326
Setting a restrictive security policy for the data collector 326
Manual changes to application server configuration for the data collector 327
Restoring the application server configuration from a backup 327
Manually configuring the data collector to monitor an application server instance 329
Manually removing data collector configuration from an application server instance 335
Customizing request information mapping . .. 337
XML file syntax 338
Enabling a request mapper 347
Request mapper type names, input, and output data 347
Example request mapper definitions. 348
Starting and stopping the monitoring environment 351
Disabling and re-enabling a data collector . .. 351
Restarting the application server 351
Starting the application server. 353
Stopping the application server 354

Part 3. Configuring data collector for WebSphere Message Broker environments 357

Chapter 9. Configuring data collection: WebSphere Message Broker 359
Upgrading to the Data Collector for WebSphere Message Broker 360
WebSphere Message Broker configuration utility 365
Enabling data collection 365
Integrating the data collector with ITCAM for SOA and ITCAM for Transactions 368
Disabling data collection 369
Disabling data collection on message flows .. 371

Part 4. Configuring ITCAM for SOA-specific data collectors for runtime environments 373

Chapter 10. Overview 375
Permissions needed to configure for data collection 376
Running the Data Collector Configuration utility 378
ConfigDC script options. 378
Running the Data Collector Configuration utility graphical user interface 379
Running the Data Collector Configuration utility in console mode 381
Running the Data Collector Configuration utility in silent mode 382
Additional configuration options 392
Running the KD4configDC script. 392
Getting help for KD4configDC 394
Configuring data collection for your environment 394

Chapter 11. Configuring data collection: Microsoft .NET 395
Using the ITCAM for Microsoft Applications .NET data collector 396
Using the ITCAM for SOA .NET data collector .. 397
Enabling data collection 397
Disabling data collection 398

Chapter 12. Configuring data collection: BEA WebLogic Server. .. 399
About Apache Axis 399
BEA client side configuration 399
BEA server side configuration 400
Enabling data collection in a single server environment. 401
Using the Data Collector Configuration utility 401
Using the KD4configDC command 403
Disabling data collection in a single server environment. 404
Using the Data Collector Configuration utility 404
Using the KD4configDC command 404
Enabling data collection in a BEA WebLogic multi-server environment 405
Disabling data collection in a BEA WebLogic multi-server environment 406
Apache Axis Limitations 408
Additional considerations 408

Chapter 13. Configuring data collection: JBoss. 409
Enabling data collection 409
Enabling data collection for JBoss V4 environments using the Data Collector Configuration utility 409
Enabling data collection using the `KD4ConfigDC` command 410
Disabling data collection 412

Disabling data collection for JBoss V4 environments using the Data Collector Configuration utility 413
Disabling data collection using the KD4ConfigDC command 413
Additional considerations 414

Chapter 14. Configuring data collection: CICS Transaction Server.. 415

Chapter 15. Configuring data collection: SAP NetWeaver 417
Enabling data collection 418
All server applications under a SAP system ID 418
A server application not located under a SAP system ID 420
A standalone client application not under a SAP system ID 421
A Web services client packaged in its own JAR file 423
A deployable client application 424
Enabling data collection using the KD4configDC command 424
Disabling data collection 426
Disabling data collection using the KD4configDC command. 427
Additional considerations 429

Chapter 16. Configuring data collection: WebSphere Community Edition 431
Enabling WebSphere CE applications for data collection. 431
Running the KD4configDC command 432
Enabling data collection manually 435
Disabling data collection 438
Running the KD4configDC command 439
Disabling data collection manually 440
Additional considerations 440

Chapter 17. Configuring data collection: DataPower SOA Appliance . 441
The DataPower data collector as a proxy 442
Planning for deployment 443
Aggregation. 444
Deployment steps 444
Unconfiguration steps 445
Configuring the DataPower SOA appliance for monitoring 445
Upgrading the DataPower firmware version .. 445
Configuring a user account on the DataPower SOA appliance 445
Configuring the XML Management Interface 446
Configuring DataPower Processing Rules . .. 447
Enabling data collection 459
The DataPower configuration file. 459
Enabling data collection using the Data Collector Configuration utility. 461
Enabling data collection using the KD4configDC command 463
Disabling data collection 473
Upgrading the data collector 473
Disabling data collection using the Data Collector Configuration utility. 473
Disabling data collection using the KD4configDC command. 474
Starting and stopping the data collector 474
Running the DataPower data collector as a Windows service or UNIX daemon 475
Registering the DataPower data collector as a Windows service or UNIX daemon 475
Starting the registered DataPower data collector 476
Stopping the registered DataPower data collector 476
Removing the DataPower data collector from the list of Windows services 477
Error handling 478
Modifying the minimum and maximum JVM heap size. 478
Configuring the requester identity type for fault monitoring 479
Configuring the aggregation of metrics in the Service Inventory Requester Identity table. . .. 480
Communicating between data collector and appliance. 480
Optimizing performance. 481
Limitations 482
Troubleshooting 482
Communication failures 483
Synchronizing time between computer systems 483
Password problems 483
Logging and Tracing 483
(Optional) Verifying that the configuration of the data collector 484
Verifying that the DataPower data collector is configured and started 484
Verifying that the DataPower appliance is storing transaction data 485
Verifying that metric log files are generated .. 486
Verifying that web service proxy is configured correctly 486
Verifying that the multi-protocol gateways are configured correctly 486
Displaying the DataPower Console interface . .. 487
Considerations when displaying the DataPower Console view 488

Chapter 18. Integrating with ITCAM for Transactions. 489
Enabling the interface to ITCAM for Transactions 490
Disabling the interface to ITCAM for Transactions 492

Part 5. Completing your installation 495

Chapter 19. Enabling historical data collection 497

Chapter 20. Installing Discovery Library Adapters 503

Chapter 21. Installing ITCAM for SOA Tools 505

Chapter 22. Installing ITCAM for SOA reports 507

Chapter 23. Configuring Tivoli Monitoring to forward events 509

Event Integration with WebSphere Service Registry and Repository 510

Chapter 24. Verifying the installation and configuration 511

Verifying the properties file. 511

Verifying Tivoli Monitoring components 512

Optional: Configuring the ITCAM for SOA monitoring agent 512

Starting and stopping the monitoring agent . .. 513

Generating initial metric log files 514

Verifying Tivoli Enterprise Portal workspaces. .. 516

Part 6. Appendixes 519

Appendix. Accessibility 521

Index 523

Trademarks 527

Notices 529

Privacy policy considerations 530

About this publication

IBM® Tivoli® Composite Application Manager for SOA, version 7.2 fix pack 1 delivers a comprehensive solution for managing services in a service-oriented architecture (SOA) running on application servers. ITCAM for SOA monitors message traffic and performs simple control of messages flowing between services in the SOA.

The *IBM Tivoli Composite Application Manager for SOA Installation Guide* provides information about installing monitoring agent functions to monitor services on Microsoft Windows, Linux, AIX®, HP-UX, and Solaris computers.

What this publication contains

This publication is divided into four main parts, containing the following chapters:

- Part 1 describes the procedures for upgrading or installing the IBM Tivoli Composite Application Manager for SOA product into the Tivoli Monitoring environment, and includes these chapters:
  - Chapter 1, “Planning an installation,” on page 3:

    Provides information to help you plan for the deployment, installation, upgrade, and update of the product on supported operating systems.
  - Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35:

    Provides instructions on installing monitoring agent application support for the components of Tivoli Monitoring, including Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal desktop client on a Windows systems.

    Provides instructions on installing or upgrading the monitoring agent on distributed Windows computer systems where services are to be monitored. This procedure assumes that components of Tivoli Monitoring are installed on other computers in your environment.

    Provides instructions on installing the ITCAM for SOA agent using a silent installation, uninstalling the agent, and installing language support.
  - Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77:

    Provides instructions on installing monitoring agent application support for the components of Tivoli Monitoring, including Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal desktop client on Linux and UNIX systems.

    Provides instructions on installing or upgrading the monitoring agent on distributed Linux and UNIX computer systems where services are to be monitored. This procedure assumes that components of Tivoli Monitoring are installed on other computers in your environment.

    Provide instructions on installing the IBM Tivoli Composite Application Manager for SOA agent using a silent installation, uninstalling the agent, and installing language support.
  - Chapter 4, “Configuring topology support on Windows systems,” on page 111

Provides information about running the SOA Domain Management Server Configuration utility to configure SOA Domain Management Server and Tivoli Common Object Repository topology support on Windows systems.

Provides instructions for installing the Tivoli Common Object Repository database, which is populated with data from one or more discovery library adapters. This data is then displayed in topology views in the Tivoli Enterprise Portal.

- Chapter 5, "Configuring topology support on Linux systems," on page 175

  Provides information about running the SOA Domain Management Server Configuration utility to configure SOA Domain Management Server and Tivoli Common Object Repository topology support on Linux and UNIX systems.

  Provides instructions for installing the Tivoli Common Object Repository database on Linux or UNIX systems.

- Chapter 6, "Installing the ITCAM for SOA SDMS agent," on page 229:

  Provides instructions on installing the ITCAM for SOA SDMS agent on Windows, Linux, and UNIX systems.

- Part 2 describes the procedures for enabling and disabling data collection for a WebSphere® Application Server environment and for performing advanced configuration tasks. Refer to these chapters for details:
  - Chapter 7, "Configuring data collection: WebSphere Application Server," on page 257
  - Chapter 8, "Advanced configuration and customization of the ITCAM Data Collector for WebSphere," on page 321
- Part 3 describes the procedures for enabling and disabling data collection for a WebSphere Message Broker environment. Refer to Chapter 9, "Configuring data collection: WebSphere Message Broker," on page 359 for details.
- Part 4 describes the procedures for enabling and disabling data collection for the various runtime environments supported with this version. It also provides instructions for integrating the .NET and DataPower® ITCAM for SOA data collectors with ITCAM for Transactions. Refer to these chapters for details:
  - Chapter 10, "Overview," on page 375
  - Chapter 11, "Configuring data collection: Microsoft .NET," on page 395
  - Chapter 12, "Configuring data collection: BEA WebLogic Server," on page 399
  - Chapter 13, "Configuring data collection: JBoss," on page 409
  - Chapter 14, "Configuring data collection: CICS Transaction Server," on page 415
  - Chapter 15, "Configuring data collection: SAP NetWeaver," on page 417
  - Chapter 16, "Configuring data collection: WebSphere Community Edition," on page 431
  - Chapter 17, "Configuring data collection: DataPower SOA Appliance," on page 441
  - Chapter 18, "Integrating with ITCAM for Transactions," on page 489
- Part 5 includes additional information you need to complete the basic installation steps and verify the configuration. See these chapters for appropriate information:
  - Chapter 19, "Enabling historical data collection," on page 497
  - Chapter 20, "Installing Discovery Library Adapters," on page 503
  - Chapter 21, "Installing ITCAM for SOA Tools," on page 505
  - Chapter 22, "Installing ITCAM for SOA reports," on page 507

- Chapter 23, “Configuring Tivoli Monitoring to forward events,” on page 509
- Chapter 24, “Verifying the installation and configuration,” on page 511

Intended audience

This guide is for services architects and services application support personnel who install IBM Tivoli Composite Application Manager for SOA to monitor and manage services in a service-oriented architecture (SOA) environment on distributed Microsoft Windows, Linux, AIX, HP-UX, and Solaris systems. The installation tasks require a working knowledge of these operating systems, and a basic knowledge of networking.

Users of this publication should be familiar with these topics:

- Monitoring concepts
- Commonly shared components of IBM Tivoli Management Services
- Tivoli Enterprise Portal user interface
- Tivoli Monitoring 6.2.3 environment
- Services that you want to monitor, including web services and services running in an enterprise service bus environment, such as DataPower, WebSphere Message Broker, or SCA applications.

Publications

This section lists publications in the product library and other related documents. It also describes how to access Tivoli publications online and how to order Tivoli publications.

ITCAM for Applications library

The following publications are included in the ITCAM for Applications library, available in the ITCAM for Applications Information Center:

- *IBM Tivoli Composite Application Manager for SOA Installation Guide*

  Provides an overview of the IBM Tivoli Management Services environment and the planning information and procedures you need to install and upgrade the application support files and the monitoring agent in a distributed operating system environment.

  This guide also includes procedures for configuring support for the service-to-service topology function, including creating databases and configuring SOA Domain Management Server and Tivoli Common Object Repository in your Tivoli Enterprise Portal Server environment.

  This guide also includes procedures for enabling and disabling the various supported runtime environments for data collection by the ITCAM for SOA, version 7.2 and later monitoring agent, and optional administrative tasks to further configure your installation.
- *IBM Tivoli Composite Application Manager for SOA User's Guide*

  Provides information on monitoring and managing resources in the Tivoli Enterprise Portal environment, including details about Take Action commands, situations, workspaces and views, including service-to-service topology workspaces and views. Some problem determination information about the various components of ITCAM for SOA is also provided, as well as information about log files and informational, warning, and error messages. This publication complements the Tivoli Enterprise Portal online help information for this monitoring agent.

- *IBM Tivoli Composite Application Manager for SOA Tools*

  Provides information about installing and using the IBM Web Services Navigator, an Eclipse based plugin for extracting services information that has been collected by monitoring agents and stored, either locally or in a historical database. This tool provides the capability to retrieve historical metric data from a connected database, or assemble several locally stored metric and content log files, and display the resulting data in several views to assist a services architect in visualizing relationships between services.
- *IBM Tivoli Composite Application Manager for Discovery Library Adapters Guide*

  Provides information about installing and running the following discovery library adapters (DLAs) provided with ITCAM for SOA: WebSphere Service Registry and Repository Discovery Library Adapter, Business Process Execution Language for Web Services Discovery Library Adapter, and IBM Tivoli Composite Application Manager for SOA Discovery Library Adapter.
- *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*

  Provides information about recovering from problems that you might encounter while installing, configuring, and using the product. Typical problem scenarios are described, and recovery procedures are provided. Error messages for the product are also documented in this guide.
- *IBM Tivoli Composite Application Manager for SOA WSRR Integration Guide*

  Provides information about integrating ITCAM for SOA version 7.2 and later with WebSphere Services Registry and Repository version 7.5 or later. The procedure for subscribing to WSRR events related to service-level definitions and the procedure for creating and deploying an SDMS configuration file is documented. The configuration file defines the rules for processing WSRR events in SDMS. Based on these rules, situations are automatically created, updated, or deleted by IBM Tivoli Monitoring when a lifecycle changes notification is received from WSRR.
- *IBM Tivoli Composite Application Manager for SOA BPM Monitoring Deployment Guide*

  Provides information about implementing an IBM BPM monitoring solution.
- *IBM Tivoli Composite Application Manager for SOA Reports Guide*

  Provides information about installing and using ITCAM for SOA Reports.

Related publications

The following documentation also provides useful information:

- IBM Tivoli Documentation Central:

  Information about IBM Tivoli Documentation is provided on the following website:

  https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli Documentation Central
- IBM WebSphere Application Server:

  Information about IBM WebSphere Application Server is provided on the following website:

  http://www.ibm.com/software/webservers/appserv/was/library/
- ITCAM for Application Diagnostics library:

  Information about ITCAM for Application Diagnostics Managing Server is provided on the following website:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp?topic=%2Fcom.ibm.itcamfad.doc_7101%2Fic-homepage.html

- IBM DB2®:

  Information about IBM DB2 is provided on the following website:

  http://www.ibm.com/software/data/sw-library/
- IBM SmartCloud® Application Performance Management UI:

  The *IBM SmartCloud Application Performance Management User Interface User's Guide* is available from the SmartCloud Application Performance Management information center at the following URL:

  http://pic.dhe.ibm.com/infocenter/tivihelp/v63r1/index.jsp?topic=%2Fcom.ibm.apm.doc_7.6%2Fapm_ui_docs%2Fapmui_76%2Ffac_landing_user.html
- IBM Application Performance Diagnostics Lite:

  The *Application Performance Diagnostics Lite Installation Guide* and the *Application Performance Diagnostics User's Guide* are available from the Application Performance Diagnostics wiki at the following URL:

  https://www.ibm.com/developerworks/community/files/app#/folder/a7149629-cdcb-41cc-a180-7bc84dc4ba5a
- ITCAM for Transactions

  Information about ITCAM for Transactions is provided on the following website:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp?topic=%2Fcom.ibm.itcamt.doc_7.3.0.1%2Fic-homepage.html

Accessing terminology online

The IBM Terminology website consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology .

Accessing publications online

The documentation CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Documentation Central website at https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli Documentation Central

Tip: If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at: http://www.ibm.com/e-business/weblink/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to http://www.ibm.com/e-business/weblink/publications/servlet/pbi.wss

2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see "Accessibility," on page 521.

Application Performance Management community on Service Management Connect

Connect, learn, and share with Service Management professionals: product support technical experts who provide their perspectives and expertise.

Access Service Management Connect at https://www.ibm.com/developerworks/servicemanagement/apm/index.html. Use Service Management Connect in the following ways:

- Become involved with transparent development, an ongoing, open engagement between other users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
- Connect one-on-one with the experts to collaborate and network about Tivoli and the Application Performance Management community.
- Read blogs to benefit from the expertise and experience of others.
- Use wikis and forums to collaborate with the broader user community.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education website:

http://www.ibm.com/software/tivoli/education/

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users. For more information about Tivoli Users Group, see www.tivoli-ug.org.

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online

Access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html .

Troubleshooting Guide
For more information about resolving problems, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*.

Conventions used in this publication

This publication uses several conventions for special terms and actions, and operating system-dependent commands and paths.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multi-column lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Words defined in text
- Emphasis of words to signify importance
- New terms in text (except in a definition list)
- Variables and values you must provide

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

The direction of the slash for directory paths might vary in this documentation. No matter which type of slash you see in the documentation, use the following guidelines for a slash:

- If using Linux, AIX, HP-UX, or Solaris operating systems, use a forward slash (/).
- If using Windows operating systems, use a backslash (\).

The names of environment variables are not always the same in Windows, Linux, AIX HP-UX, or Solaris operating systems. For example, %TEMP% in Windows is equivalent to $tmp in Linux, AIX, HP-UX, and Solaris operating systems.

For environment variables, use the following guidelines:

- If using Linux, AIX, HP-UX, or Solaris operating systems, use $*variable*.
- If using Windows operating systems, use %*variable*%.

Tip: If you are using the bash shell on a Windows operating system, you can use the Linux, AIX, HP-UX, or Solaris operating system conventions.

Resolving directory path variables

This section describes directory path naming conventions used in this guide.

The IBM Tivoli Monitoring home directory

Throughout this guide, reference is made to the *ITM_home* variable, which is the directory location where IBM Tivoli Monitoring is installed. These are the default operating system dependent values for this variable:

- For Windows: `C:\IBM\ITM`
- For Linux, HP-UX, AIX, and Solaris: `/opt/IBM/ITM`

If you installed IBM Tivoli Monitoring in a different directory location, substitute your install path location for *ITM_home*.

The IBM Tivoli Composite Application Manager for SOA home directory

Throughout the product library, reference is made to the *ITCAM4SOA_Home* variable, which is the directory location where IBM Tivoli Composite Application Manager for SOA monitoring agent is installed in the IBM Tivoli Monitoring environment. These are the default operating system dependent values for this variable:

- For Windows systems: *ITM_home*`\TMAITM6`
- For Linux, HP-UX, AIX, and Solaris systems: *ITM_home*`/`*platform*`/d4`

The ITCAM Data Collector for WebSphere home directory

Throughout the product library, reference is made to the *DC_home* variable, which is the directory location where ITCAM Data Collector for WebSphere is installed in the IBM Tivoli Monitoring environment. These are the default operating system dependent values for this variable:

- For Windows systems: *ITM_home*`\dchome\`*DC_version*
  For example: `C:\IBM\ITM\dchome\7.2.0.0.4`
- For Linux, HP-UX, AIX, and Solaris systems: *ITM_home*`/dchome/`*DC_version*
  For example: `/opt/IBM/ITM/dchome/`*DC_version*

Reference is also made to the *AppServer_home* directory, which is the directory where the WebSphere Application Server core product files are installed. For example:

- On Windows systems: `C:\Program Files\IBM\WebSphere\AppServer`
- On Linux and UNIX systems: `/opt/IBM/WebSphere/AppServer`

The Data Collector for WebSphere Message Broker home directory

Throughout the product library, reference is made to the *MB_DC_home* variable, which is the directory location where Data Collector for WebSphere Message Broker is installed in the IBM Tivoli Monitoring environment. These are the default operating system-dependent values for this variable:

- For Windows systems: *ITM_home*`\TMAITM6\k3`
  For example: `C:\IBM\ITM\TMAITM6\k3`
- For Linux, HP-UX, AIX, and Solaris systems: *ITM_home*`/`*platform_code*`/k3`
  For example: `/opt/IBM/ITM/aix533/k3`

Determining the *platform* value in directory paths

Throughout this product library, reference is made to the *platform* variable, which is part of the Linux or UNIX directory path specification for certain files that you need to access, for example:

```
ITM_home/platform/product
```

In this example, the two-character *product* variable is also part of the directory path, and is typically specified as `cq`, `d4`, or `iw` in this guide. The *product* variable for ITCAM for SOA is `d4`.

On supported Linux and UNIX operating systems, you can find the value for *platform* with this short procedure:

1. From a command prompt, navigate to the *ITM_home*/`bin` directory.
2. Run the following command:
   ```
   ./cinfo -d
   ```
3. Locate the line for product code *product*, for example:

   cq Locate this product code when you are looking up the *platform* value for Tivoli Enterprise Portal Server.

   iw Locate this product code when you are looking up the *platform* value for Tivoli Enterprise Portal Server Extension.

   d4 Locate this product code when you are looking up the *platform* value for the IBM Tivoli Composite Application Manager for SOA monitoring agent.

   The platform designation is found under the *Platform* column.

The platform designation depends on the operating system, the computer type, and the version of IBM Tivoli Monitoring that is installed. The platform for the `d4` product code is typically not the same as for the `cq` and `iw` product codes.

The following example shows the output of the **`cinfo`** command when ITCAM for SOA version 7.2 Fix Pack 1 and IBM Tivoli Monitoring version 6.2.3 are installed on a supported AIX operating system:

```
"ProdCode","Description","Platform","Version","Release"

"ax","IBM Tivoli Monitoring Shared Libraries","aix523","06220200","100"

"ax","IBM Tivoli Monitoring Shared Libraries","aix526","06220200","100"

"ax","IBM Tivoli Monitoring Shared Libraries","aix533","06230000","100"

"ax","IBM Tivoli Monitoring Shared Libraries","aix536","06230000","100"

"cq","Tivoli Enterprise Portal Server","aix536","06230000","100"

"cw","Tivoli Enterprise Portal Browser Client","aix536",
"06230000","100"

"d4","IBM Tivoli Composite Application Manager for SOA","aix523",
"07200100","100"

"gs","IBM GSKit Security Interface","aix523","07402700","100"

"gs","IBM GSKit Security Interface","aix526","07402700","100"

"hd","Warehouse Proxy","aix536","06230000","100"

"iu","IBM HTTP Server","aix536","07000000","100"
```

```
"iw","IBM Tivoli Enterprise Portal Server Extensions","aix536",
"07001500","100"

"jr","Tivoli Enterprise-supplied JRE","aix523","05120100","100"

"jr","Tivoli Enterprise-supplied JRE","aix526","05120100","100"

"kf","IBM Eclipse Help Server","aix533","06230000","100"

"ms","Tivoli Enterprise Monitoring Server","aix536","06230000","100"

"pa","Tivoli Performance Analyzer","aix533","06230000","100"

"sh","Tivoli Enterprise Monitoring SOAP Server","aix536",
"06230000","100"

"sy","Summarization and Pruning Agent","aix536","06230000","100"

"t1","File Transfer Enablement","aix536","07300000","000"

"ue","Tivoli Enterprise Services User Interface Extensions",
"aix536","06230000","100"

"ui","Tivoli Enterprise Services User Interface","aix523",
"06220200","100"

"ui","Tivoli Enterprise Services User Interface","aix526",
"06220200","100"

"ui","Tivoli Enterprise Services User Interface","aix533",
"06230000","100"

"ui","Tivoli Enterprise Services User Interface","aix536",
"06230000","100"
```

This example shows the following information:

- aix536 is the platform for Tivoli Enterprise Portal Server (product code cq)
- aix523 is the platform for the ITCAM for SOA monitoring agent (product code d4)
- aix536 is the platform for Tivoli Enterprise Portal Server Extensions (product code iw)

Part 1. Installing the product

This part of the guide describes the procedures for installing or upgrading the IBM Tivoli Composite Application Manager for SOA product, referred to here as ITCAM for SOA, into the Tivoli Monitoring environment, including:

- Planning for installation, including system requirements, database support, an overview of the installation process, and certain considerations to keep in mind
- Installing or upgrading application support for distributed Tivoli Monitoring components
- Installing or upgrading the ITCAM for SOA monitoring agent on computer systems in your environment where services are being monitored
- Installing an ITCAM for SOA SDMS agent. The agent is required if you want to view ITCAM for SOA data in the Business Process Monitoring dashboard in IBM SmartCloud Application Performance Management version 7.6 or later.
- Configuring additional support for the service-to-service topology function, including configuring SOA Domain Management Server and Tivoli Common Object Repository in your Tivoli Enterprise Monitoring Server environment

Chapter 1. Planning an installation

In ITCAM for SOA, there are three types of installation scenarios available: a pristine installation, an upgrade installation, and an update installation. An ITCAM for SOA installation is considered a pristine installation if no previous version of ITCAM for SOA is installed. A product installation is considered an upgrade installation if you installed an older version of ITCAM for SOA. A product installation is considered an update installation if you are upgrading to a later maintenance level of ITCAM for SOA.

The following sections provide an overview of the ITCAM for SOA components and describe the prerequisites for either installing, upgrading, or updating the ITCAM for SOA agent in an IBM Tivoli Monitoring environment.

Important:

- In no previous version of ITCAM for SOA is installed, you can install ITCAM for SOA version 7.2 Fix Pack 1.
- If ITCAM for SOA version 7.2 is installed, you can update your installation to ITCAM for SOA version 7.2 Fix Pack 1.
- In ITCAM for SOA version 7.1.1 is installed, you must upgrade to ITCAM for SOA version 7.2 before you update to version 7.2 Fix Pack 1.

Overview

ITCAM for SOA provides software and integrated tools to monitor, manage, and control the web services layer of the information technology architecture. ITCAM for SOA tracks the performance of web service requests through application servers that are provided by IBM, such as WebSphere Application Server and WebSphere Message Broker, and application servers that are provided by other sources, such as SAP NetWeaver and JBoss.

Figure 1 on page 4 shows all of the components of ITCAM for SOA that are described in this guide. To view an architecture diagram of all of the components in an ITCAM for SOA deployment, see the overview section of the *IBM Tivoli Composite Application Manager for SOA User's Guide.*

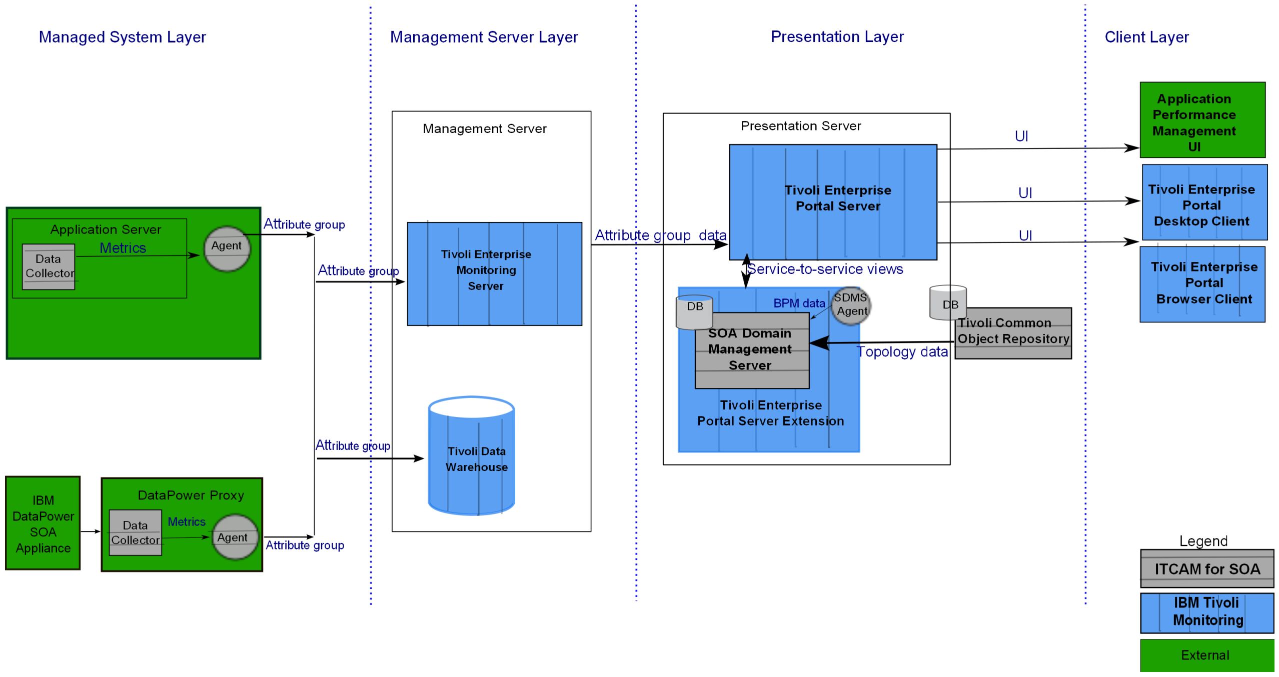


Figure 1. ITCAM for SOA components

IBM Tivoli Monitoring

Tivoli Monitoring components must be installed and configured in your environment before you install ITCAM for SOA. With Tivoli Monitoring, a user can complete the following tasks:

- Monitor for alerts on the managed systems
- Trace the causes leading up to an alert
- Monitor processing time for various requests within applications server environments
- Establish your own performance thresholds
- Create custom situations, which are conditions that Tivoli Monitoring automatically monitors
- Create and send commands to control system monitoring with the Take Action feature
- Create comprehensive reports about system conditions
- Define your own queries, with the attributes that are part of the monitoring agent, to monitor conditions of particular interest to you

Tivoli Monitoring includes the following components:

Tivoli Enterprise Monitoring Server (monitoring server)

The collection and control point for the performance and availability data and alerts that are received from the monitoring agents. The monitoring server also tracks the online and offline status of monitoring agents. In large-scale environments, a number of monitoring servers can be included to distribute load. One monitoring server is designated as the hub monitoring server, and all other monitoring servers are referred to as remote monitoring servers. For more information about installing and configuring monitoring servers, see the *IBM Tivoli Monitoring: Installation and Setup Guide.*

Tivoli Enterprise Portal Server (portal server)
Provides the core presentation layer for retrieval, manipulation, and pre-formatting of data. The portal server retrieves data from the hub monitoring server and sends the data to the portal client for presentation.

Tivoli Enterprise Portal
Supports two modes of operation; a desktop client or a web browser, both of which provide a monitoring UI.

(Optional) Tivoli Data Warehouse
Used for storing historical data that is collected from the monitoring agent. To aggregate and prune data, you must also install the Summarization and Pruning Agent.

(Optional) Tivoli Common Reporting
Used to gather, analyze, and report trends in your managed system environments. A set of predefined reports for ITCAM for SOA are part of the product.

The Tivoli Monitoring components are controlled using the Manage Tivoli Enterprise Monitoring Services utility.

For details about the capabilities of Tivoli Monitoring, and information about deploying the Tivoli Monitoring infrastructure, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Monitoring agents

The ITCAM for SOA monitoring agent interacts with the supported managed application servers and infrastructure. The monitoring agent reads data that is stored in log files that are created by the data collectors that are installed into each monitored environment. The monitoring agent forwards the data to the monitoring server and, if historical data collection is configured, to the Tivoli Data Warehouse for storing.

The monitoring agent is installed on each computer where one or more application server runtime environments are located. For DataPower environments, the monitoring agent is installed where the DataPower proxy data collector is to be located.

The ITCAM for SOA SDMS agent is provided as part of an ITCAM for SOA 7.2 Fix Pack 1 or later installation. The agent is required only if you want to view Business Process Management monitoring data in the IBM SmartCloud Application Performance Management UI version 7.6 or later.

The ITCAM for SOA SDMS agent can remotely query SOA Domain Management Server data, so you can install the agent on a separate system from the Tivoli Enterprise Portal Server.

Application support files are included with the monitoring agents. When these application support files are installed, they enable interaction with Tivoli Monitoring. Install the application support files on the computer systems where the Tivoli Monitoring components are installed

ITCAM for SOA-specific Data Collectors

Some of the data collectors that are provided with ITCAM for SOA are used by the ITCAM for SOA component only. A common set of configuration utilities are used to configure the data collectors. The ITCAM for SOA-specific data collectors monitor the web services layer of the following application server environments and appliances:

- BEA WebLogic Server
- JBoss
- CICS® Transaction Server
- SAP NetWeaver
- WebSphere Community Edition
- DataPower SOA Appliance
- Microsoft .NET

The data collectors are installed into an application server runtime environment to intercept web service calls. The data collectors store the statistical data that is collected in one or more log files on the managed system. The data collectors are installed, upgraded, or updated automatically as part of the installation, upgrade, or update of the ITCAM for SOA agent.

The data collectors are configured using the Data Collector Configuration utility in GUI mode, console mode, or silent mode, or with the `KD4configDC` script.

Data Collectors shared with other products

Some of the data collectors that are provided with ITCAM for SOA are shared with other products.

- The data collector that monitors WebSphere Application Servers, the ITCAM Data Collector for WebSphere, is shared with the following products.
  - ITCAM for SOA
  - ITCAM Agent for WebSphere Applications
  - ITCAM for WebSphere Application Server
  - ITCAM for Transactions
  - IBM Application Performance Diagnostics Lite

  You configure data collection using the ITCAM Data Collector for WebSphere configuration utilities in console mode or in silent mode. For more information about ITCAM Data Collector for WebSphere, see "ITCAM Data Collector for WebSphere" on page 7.
- The data collector that monitors WebSphere Message Broker environment, Data Collector for WebSphere Message Broker, is shared with ITCAM for Transactions. You configure the data collector using the `configDC` utility that is provided in the `bin` directory of the Data Collector for WebSphere Message Broker home directory. For more information about Data Collector for WebSphere Message Broker, see "Data Collector for WebSphere Message Broker" on page 7.
- If you want to monitor web services in Microsoft .NET version 4.0, you use ITCAM for Microsoft Applications .NET Data Collector version 7.3.1. If you want to monitor web services in Microsoft .NET version 3.5 or earlier, either use ITCAM for Microsoft Applications .NET Data Collector version 7.3.1 for data collection or the ITCAM for SOA version 7.2 Fix Pack 1 or later .NET data collector. For more information, see Chapter 11, "Configuring data collection: Microsoft .NET," on page 395.

Data Collector for WebSphere Message Broker

Beginning with ITCAM for SOA version 7.2 Fix Pack 1, a new data collector, Data Collector for WebSphere Message Broker, is provided for monitoring WebSphere Message Broker environments. The data collector is a shared component of ITCAM for Transactions version 7.3 and later and ITCAM for SOA version 7.2 Fix Pack 1 and later.

A new configuration utility, Data Collector for WebSphere Message Broker `ConfigDC` utility, is provided for enabling and disabling data collection.

ITCAM Data Collector for WebSphere

Beginning with ITCAM for SOA version 7.2, ITCAM Data Collector for WebSphere is introduced to monitor the web services layer of WebSphere Application Servers.

The data collector monitors the following WebSphere servers:

- WebSphere Application Server (Base and Network Deployment)
- WebSphere Enterprise Service Bus
- IBM Business Process Manager

The data collector is shared with the following products:

- ITCAM for SOA version 7.2 and higher
- ITCAM Agent for WebSphere Applications version 7.2 and higher
- ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 and higher
- ITCAM for Transactions version 7.3.0.1 and higher
- IBM Application Performance Diagnostics Lite

When you update to ITCAM for SOA version 7.2.0.1, if you do *not* have an earlier version of ITCAM Data Collector for WebSphere installed, you install the data collector after you update the monitoring agent. Using the ITCAM Data Collector for WebSphere Configuration utility, you can integrate the data collector with the following components:

- ITCAM Agent for WebSphere Applications monitoring agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for SOA monitoring agent
- Tivoli Performance Viewer
- IBM Application Performance Diagnostics Lite
- ITCAM for Transactions

When you update to ITCAM for SOA version 7.2.0.1, if you have an earlier version of ITCAM Data Collector for WebSphere installed, the installer skips the installation of the data collector. After you update the monitoring agent, you must migrate the data collector.

Integrating with ITCAM Agent for WebSphere Applications monitoring agent

The ITCAM Agent for WebSphere Applications monitoring agent collects information from the data collector, and processes and aggregates it for presentation to the user. The monitoring agent sends monitoring information to the Tivoli Enterprise Monitoring Server.

If you are enabling data collection for ITCAM Agent for WebSphere Applications, you can integrate the data collector with ITCAM Agent for WebSphere Applications monitoring agent, or with ITCAM for Application Diagnostics Managing Server, or with both.

You might have a version of ITCAM Agent for WebSphere Applications installed and configured for applications servers in the same WebSphere profile in which you plan to configure data collection for ITCAM for SOA. Depending on whether ITCAM Agent for WebSphere Applications is configured, complete these steps:

- If ITCAM Agent for WebSphere Applications version 7.2 is configured for the same WebSphere profile, and the data collector is at the same maintenance level, reuse the data collector installation.
- If ITCAM Agent for WebSphere Applications version 7.2 is configured for the same WebSphere profile, and the data collector is at an earlier maintenance level, migrate the data collector to the latest maintenance level. Reconfigure the data collector to integrate it with ITCAM for SOA.
- If ITCAM Agent for WebSphere Applications version 7.2 is not installed, you can integrate the data collector with the ITCAM Agent for WebSphere Applications monitoring agent, or managing server, or both when you configure data collection for ITCAM for SOA. For information about the additional procedures you must complete to configure ITCAM Agent for WebSphere Applications, see the *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.
- If an older version of ITCAM Agent for WebSphere Applications is configured for the same WebSphere profile, you must migrate the data collector before you configure data collection for ITCAM for SOA. The data collector components of the following products must be migrated to ITCAM Data Collector for WebSphere:
  - ITCAM for WebSphere version 6.1.0.4 or later
  - WebSphere Data Collector version 6.1.0.4 or later in ITCAM for Web Resources version 6.2.0.4 or later
  - ITCAM Agent for WebSphere Application version 7.1 in ITCAM for Application Diagnostics version 7.1

  After migration, the data collector continues to communicate with the monitoring agent or managing server, or both, of the previous version of ITCAM Agent for WebSphere Applications.

For more information about installing and configuring ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

Integrating with ITCAM for Application Diagnostics Managing Server

The managing server is an optional component of ITCAM for Application Diagnostics. The managing server collects information from, and provides services to, the data collector. Through its visualization engine user interface, the managing server provides detailed diagnostics information.

If you have ITCAM for Application Diagnostics version 7.1.0.3 or later installed in your environment, you can integrate ITCAM Data Collector for WebSphere with the managing server. For information about installing and configuring the managing server, see the *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation and Customization Guide*.

Integrating the data collector with ITCAM for SOA

ITCAM for SOA provides real-time monitoring of the SOA lifecycle to ensure high availability and performance. You can integrate the data collector with the ITCAM for SOA monitoring agent.

You must install its application support files and optionally configure topology support to complete the configuration of ITCAM for SOA.

Integrating with Tivoli Performance Viewer

ITCAM for WebSphere Application Server monitors the performance of the WebSphere Application Server. PMI metrics are gathered with the data collector.

The data that ITCAM for WebSphere Application Server provides augments the data that is provided by the application server through the existing PMI statistics. The metrics collected by ITCAM for WebSphere Application Server can be viewed in the Tivoli Performance Viewer (TPV). You can access the TPV from the WebSphere Application Server administrative console.

The latest version of ITCAM for WebSphere Application Server is version 7.2 supporting WebSphere Application Server 8.5. This version includes ITCAM Data Collector for WebSphere.

You might have a version of ITCAM for WebSphere Application Server installed and configured for applications servers in the same WebSphere profile in which you plan to configure data collection for ITCAM for SOA. Depending on whether ITCAM for WebSphere Application Server is configured, complete these steps:

- If ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5 is configured for the same WebSphere profile, and the data collector is at the same maintenance level, reuse the data collector installation.
- If ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5 is configured for the same WebSphere profile, and the data collector is at an earlier maintenance level, migrate the data collector to the latest maintenance level.
- If WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5 is not installed, you can integrate the data collector with the TPV when you configure data collection for ITCAM for SOA. For information about using ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5, see the *IBM Tivoli Composite Application Manager for WebSphere Application Server 72 support for WebSphere Application Server 8.5: Installation and User Guide*.
- If ITCAM for WebSphere Application Server version 7.2 is configured for the same WebSphere profile, you must migrate the ITCAM for WebSphere Application Server data collector before you configure data collection for ITCAM for SOA. ITCAM for WebSphere Application Server version 7.2 is used to monitor WebSphere Application Server version 8.

  Important: Server monitoring that is provided by ITCAM for WebSphere Application Server in the WebSphere Administrative Console continues after the migration.

Integrating with IBM Application Performance Diagnostics Lite Data Collector

IBM Application Performance Diagnostics Lite is a tool for diagnostic investigation of applications that run on WebSphere Application Server and WebSphere Portal Server.

You might have a version of the Application Performance Diagnostics Lite data collector installed and configured for applications servers in the same WebSphere profile in which you plan to configure data collection for ITCAM for SOA. Depending on whether the Application Performance Diagnostics Lite data collector is configured, complete these steps:

- If the Application Performance Diagnostics Lite data collector is configured for the same WebSphere profile, and the data collector is at the same maintenance level, reuse the data collector installation.
- If the Application Performance Diagnostics Lite data collector is configured for the same WebSphere profile, and the data collector is at an earlier maintenance level, migrate the data collector to the latest maintenance level.
- If the Application Performance Diagnostics Lite data collector is not installed, you can integrate the data collector with the Application Performance Diagnostics Lite when configuring data collection for ITCAM for SOA. For information about using Application Performance Diagnostics Lite, see the *Application Performance Diagnostics Installation Guide*.

Integrating with ITCAM for Transactions

ITCAM for Transactions tracks transactions within and among applications. The product determines the time that is spent by the transaction in each application and, where possible, the time spent communicating between applications.

The data collector can be configured to construct and send tracking events through the Transaction Tracking Application Programming Interface (TTAPI) to the ITCAM for Transactions Transaction Collector. ITCAM for Transactions displays the aggregated transaction information and topology in workspaces.

To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli Monitoring environment.

Beginning with ITCAM for Transactions version 7.3.0.1, ITCAM Data Collector for WebSphere is provided as a component of ITCAM for Transactions.

For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.

Application support files

To enable the monitoring agents to integrate with Tivoli Monitoring, application support files that are part of ITCAM for SOA must be installed on all hub and remote monitoring servers, all portal servers, and all portal clients except browser-based clients.

Important: For the ITCAM for SOA agent, you must install the application support files provided with ITCAM for SOA version 7.2 before you install the application support files for ITCAM for SOA version 7.2.0.1.

The ITCAM for SOA application support files install and configure the following elements:

- On the monitoring server, the application support files provides data tables and situations for the ITCAM for SOA monitoring agent. The data tables are Services_Metrics and Services_Inventory.
- On the portal server, the application support files provide ITCAM for SOA workspaces.
- On the portal, the application support files provide help resources and language packs.

When self-description is enabled on the ITCAM for SOA component and on the monitoring servers, application support files are automatically installed on the monitoring servers, without the need to recycle the monitoring servers. Application support files must be manually installed on the portal server and portal client. The conditions that must be met for self-description to operate are specified in "Enabling application support through self-description" on page 36 for Windows systems and in "Enabling application support through self-description" on page 77 for Linux and UNIX systems.

SOA Domain Management Server

The SOA Domain Management Server is an optional component in ITCAM for SOA. If you want to include service-to-service topology views in the Operation Flow workspaces on the portal server in your deployment, you must configure the SOA Domain Management Server and its associated database.

The SOA Domain Management Server is used to store and retrieve information about service resources, such as application servers, service ports, operations, and the relationships between them. These service-to-service relationships and flows can then be displayed in Tivoli Enterprise Portal topology workspaces and views.

This additional component of ITCAM for SOA is installed in a runtime environment called Tivoli Enterprise Portal Server Extensions.

For more information about topology support and creating the SOA Domain Management Server database, see Chapter 4, "Configuring topology support on Windows systems," on page 111 or Chapter 5, "Configuring topology support on Linux systems," on page 175.

Tivoli Common Object Repository

The Tivoli Common Object Repository is an optional component in ITCAM for SOA. If you want to include service registry and business services integration information in topology views and workspaces in your deployment, you must configure the Tivoli Common Object Repository and the SOA Domain Management Server, and their associated databases.

The Tivoli Common Object Repository is used to integrate service registry and business process information with information about service resources. This additional component of ITCAM for SOA is installed in the Tivoli Enterprise Portal Server Extensions runtime environment.

Restriction: If you integrate ITCAM for SOA version 7.2 or later with Tivoli Monitoring 6.2.2, you must configure Tivoli Common Object Repository when you configure the SOA Domain Management Server.

For more information about configuring topology support and creating the Tivoli Common Object Repository and its database, see Chapter 4, “Configuring topology support on Windows systems,” on page 111 or Chapter 5, “Configuring topology support on Linux systems,” on page 175.

ITCAM for SOA tools

In ITCAM for SOA version 7.2 and later, ITCAM for SOA Tools consists of one component; IBM Web Services Navigator, a plug-in based on Eclipse, that can be installed into a stand-alone Eclipse environment. The component is optional. Metric information about web service request and response messages are intercepted by the ITCAM for SOA monitoring agent and data collectors. The data is written to multiple log files and stored in the Tivoli Data Warehouse, if historical data collection is enabled.

The IBM Web Services Navigator can be configured to retrieve the web services data from the data warehouse and to transform this data into a log file format to display the data in the viewer. Alternatively, the IBM Web Services Navigator can import metric log files directly and transform the data into the correct format for display in the viewer.

Discovery Library Adapters

ITCAM for SOA displays static service-to-service relationships in a graphical topology display in the portal, which you can navigate through to understand the relationships. The topology data is stored in the Tivoli Common Object Repository database. The database is populated by one or more discovery library adapters (DLAs).

A DLA is a program that extracts data from a source application and generates an XML file, referred to as a discovery library adapter book. Using a bulk load program, data that is stored in the books is loaded into the Tivoli Common Object Repository periodically.

Three discovery library adapters are provided with ITCAM for SOA:

WebSphere Service Registry and Repository DLA
Discovers the relationships between services, service ports, operations, and port types of web services that are registered in WebSphere Service Registry and Repository.

Business Process Execution Language for Web Services DLA
Discovers the relationships between port types, operations, and business processes that are based on the business processes that are defined in IBM Integration Developer and IBM WebSphere Business Modeler.

ITCAM for SOA DLA
Discovers the relationships between service ports and operations, and the application servers and computer systems on which these services are deployed, based on data that is retrieved from the monitoring server.

The data that is retrieved from the DLAs can be displayed in the Service Management workspace that is provided with ITCAM for SOA.

The books that are generated by the DLAs can also be loaded into IBM Tivoli Change and Configuration Management Database, IBM Tivoli Application Dependency Discovery Manager, and IBM Tivoli Business Service Manager.

For information about installing and configuring discovery library adapters, see *IBM Tivoli Composite Application Manager for SOA Discovery Library Adapters Guide*.

Databases

The data collectors gather monitoring and diagnostic information from the application servers. This data can be sent to the Tivoli Data Warehouse for long-term storage. The data can also be transformed in the SOA Domain Management Server database to display service-to-service topology information in the portal workspaces and views. Data that is related to registered services, business integration information, and application server names can be collected with discovery library adapters and transformed in the Tivoli Common Object Repository database for display in topology views in the portal desktop.

Tivoli Data Warehouse

The Tivoli Data Warehouse supports IBM DB2, Oracle, and Microsoft SQL Server warehouse databases for collection of historical data.

You might have to consult your local system or database administrator to set up the database if it is not already defined, or refer to your Tivoli Monitoring documentation for the procedures to follow, including these tasks:

- Creating user IDs and passwords with required authority to access the database
- Creating the warehouse database that receives historical data
- Configuring an ODBC database connection to the database
- Configuring and registering the Warehouse Proxy

Plan the size of your warehouse database to ensure that you have a large enough database server to contain your data. To find the warehouse load projection spreadsheet in the Tivoli Integrated Service Management Library search for “warehouse load projections” or the navigation code “1TW10TM1Y” at the following URL: https://www-304.ibm.com/software/brandcatalog/ismlibrary/. This spreadsheet has a tab for the ITCAM for SOA monitoring agent.

To determine which ITCAM for SOA attribute groups can be enabled for historical data collection, see Chapter 19, “Enabling historical data collection,” on page 497.

IBM Web Services Navigator can be configured to display historical information that is collected by the ITCAM for SOA monitoring agent. For more information about connecting the IBM Web Services Navigator to the Tivoli Data Warehouse, see *IBM Tivoli Composite Application Manager for SOA Tools*.

Tivoli Common Reporting can be configured to retrieve data from the Tivoli Data Warehouse for reporting. For information about connecting Tivoli Common Reporting to the Tivoli Data Warehouse database, see the IBM Tivoli Common Reporting Information Center.

SOA Domain Management Server database

If you want to display service-to-service topology flows in Operational Flow workspaces, you must configure support for SOA Domain Management Server and its associated database.

ITCAM for SOA also includes a graphical user interface configuration utility that you use to create and configure the SOA Domain Management Server database. On Windows, Linux, and UNIX operating systems, console mode and silent mode (with a response file) are also supported.

The SOA Domain Management Server database, containing information about service-to-service relationships, can be created on a supported DB2 server, a supported Microsoft SQL server (Windows systems only), or a supported Oracle server. This server can be the same database server that is used by Tivoli Enterprise Portal Server if located on the same computer as Tivoli Enterprise Portal Server, or this server can be on a separate, remote computer.

The SOA Domain Management Server Configuration utility can create these databases for you locally, or you can create them yourself on local or remote database servers with database creation scripts provided with the product. Oracle databases must be created manually. If you create your own databases manually, you still must run the SOA Domain Management Server Configuration utility on the Tivoli Enterprise Portal Server to complete the configuration of topology support.

For more information about creating databases, creating database users, and running the SOA Domain Management Server Configuration utility, see Chapter 4, “Configuring topology support on Windows systems,” on page 111 or Chapter 5, “Configuring topology support on Linux systems,” on page 175. You might have to consult your local database administrator for assistance with these tasks.

Tivoli Common Object Repository database

If you use service registry and business service integration information in your views, you must configure support for both SOA Domain Management Server and Tivoli Common Object Repository and their associated databases. You must also install and run one or more of the discovery library adapters that are provided with this product.

You can configure the SOA Domain Management Server to operate with or without the Tivoli Common Object Repository database.

You can configure the Tivoli Common Object Repository databases with the SOA Domain Management Server Configuration utility. On Windows, Linux, and UNIX operating systems, console mode, and silent mode (with a response file) are also supported.

The Tivoli Common Object Repository database can be created on a supported DB2 server or a supported Oracle server. The server can be installed on either the Tivoli Enterprise Portal Server computer or on a different, remote database server.

The SOA Domain Management Server Configuration utility can create the database for you locally, or you can create them yourself on local or remote database servers with database creation scripts that are provided with the product. Oracle databases must be created manually. If you create your own databases manually, you still have to run the SOA Domain Management Server Configuration utility on the Tivoli Enterprise Portal Server to complete the configuration of topology support.

Software and hardware prerequisites

The following sections provide specific information about the software and hardware requirements for installing ITCAM for SOA monitoring agent and Tools in a Tivoli Monitoring environment.

Required software

The software prerequisites for upgrading to ITCAM for SOA version 7.2 and installing or updating to ITCAM for SOA version 7.2 Fix Pack 1 are covered in the following sections:

Tivoli Monitoring

For Tivoli Monitoring software requirements, refer to the planning and installation information in the *IBM Tivoli Monitoring: Installation and Setup Guide* provided with Tivoli Monitoring. If you plan to write historical data to a warehouse database for later retrieval and analysis by Tivoli Enterprise Portal workspaces, the IBM Web Services Navigator or Tivoli Common Reporting, see the additional information about setting up data warehousing (including configuring the Warehouse Proxy agent and Summarization and Pruning agent).

See *IBM Tivoli Monitoring: Installation and Setup Guide* for information about the software environments that are supported by the following Tivoli Monitoring components:

- Database types that are supported by the Tivoli Data Warehouse
- Web browsers that are supported by the Tivoli Enterprise Portal
- Versions of Tivoli Common Reporting that are supported by Tivoli Monitoring

Check your Tivoli Monitoring documentation regularly for operating system patches that are required.

ITCAM for SOA software requirements

See the Software product compatibility reports website to generate various reports that are related to product and component requirements.

To view the system requirements for server-side components in ITCAM for SOA version 7.2 and later, see the Server-side components detailed system requirements report.

To view the system requirements for agent-side components in ITCAM for SOA version 7.2 and later, see the Agent-side components detailed system requirements report.

Restriction:

- On a Linux 64-bit operating system, the following set of graphical libraries must be installed in 32-bit and 64-bit for the 32- bit Java™ version to work properly:
  - libXmu
  - libXp
  - libXtst
  - libXft

  The Linux system requires these libraries to display graphics with X Window System. If these libraries are missing, the installer might not start in GUI mode.

- The ITCAM for SOA monitoring workspaces in the Tivoli Enterprise Portal do not support web browsers running Oracle Java SDKs.

Data Collector for WebSphere Message Broker cross product dependency

In ITCAM for SOA version 7.2.0.1, a new data collector, Data Collector for WebSphere Message Broker, is introduced to monitor WebSphere Message Broker environments. The data collector provides support for both 32-bit and 64-bit broker processes on various platforms.

The specific operating system and bit mode combinations that are supported by the data collector for WebSphere Message Broker version 6.1 are as follows:

Table 1. Broker processes supported by operating system by the data collector for WebSphere Message Broker version 6.1

	WebSphere Message Broker version 6.1	
Operating system	**32-bit process**	**64-bit process**
AIX	X	X
HP-UX PA-RISC	X	X
Linux on x86	X	
Linux on x86-64	X	X
Linux on System z®		X
Linux on Power®		X
Solaris SPARC	X	X
Windows 32 bit	X	

The specific operating system and bit mode combinations that are supported by the data collector for WebSphere Message Broker version 7.0 and version 8.0 are as follows:

Table 2. Broker processes supported by operating system by the data collector for WebSphere Message Broker version 7.0 and version 8.0

	WebSphere Message Broker version 7.0 and version 8.0	
Operating system	**32-bit process**	**64-bit process**
AIX		X
Linux on x86	X	
Linux on x86-64		X
Linux on System z		X
Linux on Power		X
Solaris SPARC		X
Windows 32 bit	X	
Windows 64 bit	X	X

Required hardware

Table 3 on page 17 presents the disk space and memory of the operating systems on which ITCAM for SOA version 7.2 has been validated. It also presents the memory used by the ITCAM for SOA agent on the Linux operating system.

To determine whether you require additional disk space and memory for your ITCAM for SOA version 7.2 installation, use the disk space and memory values in Table 3 as a guideline.

Note: The values in Table 3 do *not* represent the minimum disk space and memory required by ITCAM for SOA version 7.2.

Table 3. Disk space and memory of the operating systems on which ITCAM for SOA has been validated

Operating system	**Disk space**	**Memory**	**ITCAM for SOA agent memory usage**
Windows 32 bit	670 MB for the ITCAM for SOA agent product files	4 GB RAM	N/A
Windows 64 bit	660 MB for the ITCAM for SOA agent product files	4 GB RAM	N/A
Linux	790 MB for the ITCAM for SOA agent product files	10 GB RAM	531 Mb
AIX	850 MB for the ITCAM for SOA agent product files	5.4 GB RAM	N/A
Solaris	770 MB for the ITCAM for SOA agent product files	15 GB RAM	N/A
HP-UX	890 MB for the ITCAM for SOA agent product files	4 GB RAM	N/A

For information about the required hardware for the Tivoli Monitoring components, see the Tivoli Monitoring documentation.

Considerations for data collectors

As you plan to install, upgrade, or update ITCAM for SOA into your runtime environment, take the following guidelines into account:

- The computer system on which are you installing, upgrading, or updating ITCAM for SOA data collectors might already have other ITCAM for SOA data collectors enabled for other applications (or servers, depending on your runtime environment). Any combination of supported ITCAM for SOA data collector types (JBoss, DataPower, and others) can coexist on a single system. However, each ITCAM for SOA data collector type must be at the same version on any one system.
- You can enable the ITCAM for SOA data collectors for as many application server environment types as you want.
- If you plan to install, upgrade, or update an ITCAM for SOA data collector on a computer system on which other ITCAM for SOA data collectors are installed, you must disable the existing data collectors before performing the installation. You must re-enable the existing data collectors when the installation completes.

You must enable and disable the existing data collectors because some code is shared between runtime environments, specifically JBoss and BEA WebLogic Server.

Remember: The recommendation does not apply to ITCAM Data Collector for WebSphere or Data Collector for WebSphere Message Broker. These data collectors do not share code with other ITCAM for SOA data collectors.
See Part 4, “Configuring ITCAM for SOA-specific data collectors for runtime environments,” on page 373 for details on disabling and enabling your runtime environments for data collection.

- Enabling and disabling data collection requires the user to have permissions to update the application server environment. See Part 4, “Configuring ITCAM for SOA-specific data collectors for runtime environments,” on page 373 for details on the requirements for each unique application server environment.
- You must determine the following when you install ITCAM Data Collector for WebSphere for monitoring WebSphere Application Server runtime environments:
  - Whether the data collector is already configured for ITCAM Agent for WebSphere Applications, ITCAM for WebSphere Application Server, or IBM Application Performance Diagnostics Lite for application servers within the same profile.
  - Whether an ITCAM Agent for WebSphere Applications version 7.1 Data Collector, an ITCAM for WebSphere version 6.1.0.4 data collector, an WebSphere Data Collector 6.1.0.4 or later (component of ITCAM for Web Resources version 6.2), or an ITCAM for WebSphere Application Server version 7.2 Data Collector is already installed on the computer system and enabled for application servers within the same profile.
  - Whether the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector is installed on the computer system.
  - Whether a previous maintenance version of ITCAM Data Collector for WebSphere is installed.
  - Before you install ITCAM Data Collector for WebSphere for monitoring WebSphere Application Server runtime environments, review the guidelines on installing and configuring IBM Business Process Manager in “Business Process Monitoring” on page 258.
  - The installation, update, and upgrade procedures that you follow for monitoring a WebSphere Application Server environment depend on the data collectors that are already installed. For information about the installation procedures, see “Installing ITCAM for SOA 7.2, updating to 7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere” on page 261.
- If you plan to configure data collection for WebSphere Message Broker environments, determine whether the Data Collector for WebSphere Message Broker is already installed as part of ITCAM for Transactions version 7.3 or later.
  - If the data collector is installed and is at the same maintenance level, skip the steps to install and enable the data collector. Instead, integrate the data collector with the ITCAM for SOA monitoring agent by setting the `default.kd4.enabled` property in the `KK3.dc.properites` file to `true`. The `KK3.dc.properites` file is in the *MB_dc_home* `config` directory. For more information about integrating the data collector with ITCAM for SOA, see “Integrating the data collector with ITCAM for SOA and ITCAM for Transactions” on page 368.

- If the data collector is installed but is at an earlier maintenance level, install the data collector and follow the procedure for updating the maintenance level of the data collector in "Upgrading to the Data Collector for WebSphere Message Broker" on page 360.
- If an older version of the data collector is installed, follow the upgrade procedure in "Upgrading to the Data Collector for WebSphere Message Broker" on page 360.

Remember: Throughout this document, there are references to enabling applications for data collection, but for environments such as WebSphere, assume that the reference is to enabling the server.

Performing a pristine installation of ITCAM for SOA version 7.2 Fix Pack 1

The following installation procedure for the ITCAM for SOA agent assumes that, if you choose to install a data collector to monitor a WebSphere Application Server environment, that you are performing a pristine installation of the ITCAM Data Collector for WebSphere on a computer system where no previous version of the following products is installed:

- ITCAM for SOA WebSphere Application Server data collector
- ITCAM Agent for WebSphere Applications
- ITCAM for WebSphere Application Server
- IBM Application Performance Diagnostics Lite
- ITCAM for Transactions version 7.3.0.1 or later

All other procedures for installing a data collector for a WebSphere Application Server environment, introduced by the support of a shared data collector in mixed ITCAM environments, are outlined in "Installing ITCAM for SOA 7.2, updating to 7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere" on page 261.

Before installing ITCAM for SOA

Before you install ITCAM for SOA for the first time, complete the following tasks:

1. Close the Manage Tivoli Enterprise Monitoring Services utility if it is open on the application server where you are installing the monitoring agent.
2. Review the software requirements for ITCAM for SOA version 7.2 Fix Pack 1 in "Required software" on page 15.
3. Review the considerations for data collectors in "Considerations for data collectors" on page 17.
4. If you are installing a BEA WebLogic Server data collector, stop the server if the BEA WebLogic Server is running on the same computer system where you are installing the monitoring agent.
5. Install your Tivoli Monitoring environment. Install one of the minimum supported versions if one is not already installed.
6. (Optional) If you are installing ITCAM Data Collector for WebSphere, verify that the prerequisite packages for this WebSphere Application Server data collector are installed correctly before starting the installer.
   The Environment Checking Utility (ECU) generates a report of the operating-system packages and libraries installed. From the report, you can

determine if the system prerequisites are met. For more information about generating an ECU report, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*.

Installing Tivoli Monitoring

Before you install ITCAM for SOA version 7.2 Fix Pack 1 for the first time, you must install or upgrade to the minimum supported version of Tivoli Monitoring. To view the minimum supported version of Tivoli Monitoring for the ITCAM for SOA version 7.2 Fix Pack 1 agent, see the software product compatibility reports website.

If you are upgrading Tivoli Monitoring, the upgrade must be performed on each computer in your enterprise where the following components of Tivoli Monitoring are installed:

- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

Refer to your Tivoli Monitoring documentation for complete details about installing, upgrading, and configuring the Tivoli Monitoring environment.

You might also have to upgrade existing monitoring agents for other Tivoli products. For information about upgrades, refer to your monitoring agent product documentation, and check if upgrading to one of these supported versions of Tivoli Monitoring affects your existing monitoring agents.

Be sure to install or upgrade the following additional components of Tivoli Monitoring as needed:

- Tivoli Enterprise Portal web browser enablement (also referred to as the *browser client*)
- Warehouse Proxy (if you intend to use historical reporting or save historical data to a database for later retrieval and analysis with IBM Web Services Navigator, or for displaying historical data in certain ITCAM for SOA workspaces and views)
- IBM Eclipse Help Server, which is used to display searchable online help information in the IBM Eclipse Help System environment. The Help Server is installed with the Tivoli Enterprise Portal Server
- The IBM Java Runtime Environment (JRE) or the Sun JRE for running the desktop version of the Tivoli Enterprise Portal
- Internet Explorer, with the Java plug-in (at the same version as the JRE) for running the web browser version of the Tivoli Enterprise Portal

The procedures for installing and upgrading the additional Tivoli Monitoring components are documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1

To install and configure ITCAM for SOA version 7.2 Fix Pack 1, complete the following tasks:

Table 4. Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1

Steps	Description
Enable ITCAM for SOA application support for Tivoli Monitoring components.	For information about enabling application support, see the following sections: • "Enabling application support on the monitoring server, portal server, and desktop client" on page 36 on Windows systems • "Enabling application support on the monitoring server, portal server, and desktop client" on page 77 on Linux or UNIX systems
Install the ITCAM for SOA monitoring agent in an application server runtime environment.	For information about installing the ITCAM for SOA monitoring agent, see the following sections: • "Installing and upgrading the ITCAM for SOA monitoring agent and data collectors" on page 40 on Windows systems • "Installing, upgrading, or updating the monitoring agent" on page 84 on Linux or UNIX systems
To configure data collection for a WebSphere Application Server, install or migrate to the ITCAM Data Collector for WebSphere.	To install ITCAM Data Collector for WebSphere and configure data collection, see "Step 18: Install ITCAM Data Collector for WebSphere" on page 55 on Windows systems and "Installing, upgrading, or updating the monitoring agent" on page 84 on Linux and UNIX systems. If the ITCAM Data Collector for WebSphere is already installed, you must migrate the data collector to the latest maintenance level. Data collection for the application server instances is enabled as part of the migration. For information about migrating the data collector, see "Updating to V7.2 Fix Pack 1 and configuring ITCAM Data Collector for WebSphere" on page 272.
Configure the SOA Domain Management Server and the Tivoli Common Object Repository.	Run the ConfigDMS utility to configure the SOA Domain Management Server and Tivoli Common Object Repository. For information about running the ConfigDMS utility, see Chapter 4, "Configuring topology support on Windows systems," on page 111 on Windows systems or Chapter 5, "Configuring topology support on Linux systems," on page 175 on Linux and UNIX systems.
Reconfigure the Tivoli Enterprise Portal Server.	For information about reconfiguring the Tivoli Enterprise Portal Server, see "Reconfiguring and restarting the Tivoli Enterprise Portal Server" on page 173 on Windows systems or "Rebuilding and restarting the Tivoli Enterprise Portal Server" on page 227 on Linux and UNIX systems.
If you plan to send business process monitoring data to SmartCloud Application Performance Management UI, install and configure the ITCAM for SOA SDMS agent and its application support files.	For information about installing the agent, see Chapter 6, "Installing the ITCAM for SOA SDMS agent," on page 229.
Start the ITCAM for SOA monitoring agent.	For information about starting the agent, see "Starting and stopping the monitoring agent" on page 513.
Start the ITCAM for SOA SDMS monitoring agent, if installed.	For information about starting the agent, see "Starting and stopping the monitoring agent" on page 513.

Table 4. Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1 (continued)

Steps	**Description**
Enable ITCAM for SOA-specific data collectors.	Enable data collection for runtime environments, as required. For information about enabling data collection, see the following sections: • For BEA WebLogic Server, see Chapter 12, “Configuring data collection: BEA WebLogic Server,” on page 399. • For JBoss, see Chapter 13, “Configuring data collection: JBoss,” on page 409. • For CICS Transaction Server, see Chapter 14, “Configuring data collection: CICS Transaction Server,” on page 415. • For SAP NetWeaver, see Chapter 15, “Configuring data collection: SAP NetWeaver,” on page 417. • For WebSphere Community Edition, see Chapter 16, “Configuring data collection: WebSphere Community Edition,” on page 431. • For DataPower SOA Appliance, see Chapter 17, “Configuring data collection: DataPower SOA Appliance,” on page 441.
Enable Data Collector for WebSphere Message Broker.	Enable data collection for WebSphere Message Broker environments, if required. For more information about enabling data collection, see Chapter 9, “Configuring data collection: WebSphere Message Broker,” on page 359.
Integrate DataPower SOA appliance and Microsoft .NET data collectors with ITCAM for Transactions.	(Optional) Integrate the DataPower SOA appliance and Microsoft .NET data collectors with ITCAM for Transactions. For information about integrating the data collectors with ITCAM for Transactions, see Chapter 18, “Integrating with ITCAM for Transactions,” on page 489.
Enable historical data collection.	(Optional) Enable data collection for ITCAM for SOA. **Important:** After you install ITCAM for SOA version 7.2 Fix Pack 1, data is not viewable in the Tivoli Enterprise Portal until one of the following conditions occurs: • The Warehouse Proxy Agent exports its first batch of data for a specific attribute group. • The Summarization and Pruning agent runs for the first time after the install ITCAM for SOA version 7.2 Fix Pack 1. For information about enabling historical data collection, see Chapter 19, “Enabling historical data collection,” on page 497.
Install the latest version of the Discovery Library Adapters (DLAs) that are provided with ITCAM for SOA.	(Optional) Install the DLAs that populate the Tivoli Common Object Repository database with relationship information to display in Tivoli Enterprise Portal topology workspaces and views.
Install ITCAM for SOA Tools.	(Optional) Install ITCAM for SOA Tools, which includes the Web Services Navigator. To view data from Tivoli Data Warehouse in the Web Services Navigator, establish a connection to one or more supported databases where historical metric data is being stored. For information about installing ITCAM for SOA Tools, see the *IBM Tivoli Composite Application Manager for SOA Tools* guide.
Import ITCAM for SOA reports into Tivoli Common Reporting.	(Optional) Import ITCAM for SOA reports into Tivoli Common Reporting.For information about installing ITCAM for Reports, see the *IBM Tivoli Composite Application Manager for SOA Reports Guide*.
Configure Tivoli Monitoring to forward ITCAM for SOA events.	(Optional) Configure Tivoli Monitoring to forward events from ITCAM for SOA to an external destination. For information about forwarding events, see Chapter 23, “Configuring Tivoli Monitoring to forward events,” on page 509.

Table 4. Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1 (continued)

Steps	Description
Integrate ITCAM for SOA events with WebSphere Service Registry and Repository.	(Optional) Integrate ITCAM for SOA events with WebSphere Service Registry and Repository. Configure forwarding of ITCAM for SOA situations events to WebSphere Service Registry and Repository. For more information about configuring the interface between ITCAM for SOA and WebSphere Service Registry and Repository, see *IBM Tivoli Composite Application Manager for SOA WSRR Integration Guide*.
Verify that ITCAM for SOA agent is correctly installed.	For information about verifying the installation of ITCAM for SOA, see Chapter 24, “Verifying the installation and configuration,” on page 511.

Upgrading to ITCAM for SOA version 7.2

You must upgrade from ITCAM for SOA version 7.1.1 to version 7.2 before you update to version 7.2 Fix Pack 1.

Important: ITCAM for SOA version 7.2 is available from ITCAM for Applications version 7.2. For more information about ITCAM for Applications version 7.2, see the ITCAM for Applications information center.

You do not have to upgrade all of your ITCAM for SOA version 7.1.1 monitoring agents in the Tivoli Monitoring environment at the same time. During the time period when there is a mixture of version 7.1.1 and version 7.2 agents in your environment, the agents are supported at their respective levels of function.

When you upgrade ITCAM for SOA monitoring agents to version 7.2, each of the existing runtime environments for the ITCAM for SOA data collectors on that computer must be upgraded to version 7.2.

Upgrading the WebSphere Application Server data collector

When you upgrade data collection for the WebSphere Application Server, you install a new data collector for the WebSphere Application Server as part of the upgrade procedure. ITCAM Data Collector for WebSphere is a shared component between the following products:

- ITCAM for SOA
- ITCAM Agent for WebSphere Applications
- ITCAM for WebSphere Application Server
- IBM Application Performance Diagnostics Lite
- ITCAM for Transactions

When you upgrade the monitoring agent to version 7.2, you specify a directory in which to install the 7.2 version of the data collector. If the same version, release, and maintenance level of the data collector is already installed as part of the installation of another product, and is configured for the same profile in which you plan to configure data collection for ITCAM for SOA, you can reuse this data collector installation.

The procedure for upgrading the ITCAM for SOA WebSphere Application Server data collector to ITCAM Data Collector for WebSphere in the following section assumes that neither the same version nor an older version of ITCAM Data Collector for WebSphere is configured by another product for application servers in the same WebSphere profile.

The procedure for upgrading to ITCAM Data Collector for WebSphere when an older version of the data collector is configured for the same profile by another product is described in "Upgrading to V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere" on page 266.

If you intend to monitor business process applications through ITCAM for SOA, there are a number of options you must configure when installing and configuring IBM Business Process Manager. Before you upgrade ITCAM for SOA, review the guidelines on installing and configuring IBM Business Process Manager in "Business Process Monitoring" on page 258.

Upgrading ITCAM for SOA on a Solaris platform

As Oracle supports only a clean installation on Solaris 11, you cannot upgrade from ITCAM for SOA version 7.1.1 on Solaris 10 to ITCAM for SOA version 7.2 on Solaris 11. Instead, on a system where Solaris 10 and ITCAM for SOA version 7.1.1 are installed, complete these steps:

1. Create a backup of all of your data. Include any database files in your backup.
2. Perform a pristine installation of Solaris 11 on your system.
3. Restore your ITCAM for SOA version 7.1.1 configuration data on Solaris 11.
4. Upgrade from ITCAM for SOA version 7.1.1 to version 7.2

Before upgrading ITCAM for SOA

Before upgrading ITCAM for SOA, complete the following tasks:

1. Close the Manage Tivoli Enterprise Monitoring Services utility if it is open on the application server where you are installing the monitoring agent.
2. Review the software requirements for ITCAM for SOA version 7.2 in "Required software" on page 15.
3. Review the considerations for data collectors in "Considerations for data collectors" on page 17.
4. Stop all application servers on the computer where the monitoring agent is being installed.
   If you have the Microsoft .Net application server environment running on this application server, stop the `w3svc` service. For information about stopping the current version of your application servers, see your product documentation.
5. Disable (unconfigure) any existing ITCAM for SOA data collectors on this computer system that are currently at version 7.1.1 and that you plan to upgrade to version 7.2 (see "Disabling data collection for your monitoring environments" on page 25).
   You can use either the Data Collector Configuration utility (`ConfigDC`) or the `KD4ConfigDC` script to disable the ITCAM for SOA-specific data collectors.
6. Upgrade your Tivoli Monitoring environment to one of the minimum supported versions, if required (see "Upgrading Tivoli Monitoring" on page 25).
7. (Optional) If you are upgrading the data collector for WebSphere Application Servers, verify that the prerequisite packages for this WebSphere Application Server data collector are installed correctly before launching the installer.
   The Environment Checking Utility (ECU) generates a report of the operating-system packages and libraries installed. From the report, you can determine if the system prerequisites are met. For more information about generating an ECU report, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*.

Disabling data collection for your monitoring environments

Before you upgrade your current Tivoli Monitoring or ITCAM for SOA installation, be sure to disable (unconfigure) data collection for all runtime environments. You can re-enable data collection for your runtime environments when the update to version 7.2 Fix Pack 1 is complete.

For ITCAM for SOA version 7.1.1, see the multiple chapters under Part 2, Configuring for data collection, in the *ITCAM for SOA Installation Guide*, for the procedures specific to each runtime environment about disabling data collection. See the ITCAM for SOA http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.itcamsoa.doc_7.1/kd4inmst57.htm#part2Information Center.

DataPower environments:

Do not use the `–disable` option of the `KD4configDC` script or the Data Collector Configuration utility. Instead, you must complete the following steps:

1. Stop the DataPower data collector with the **`stopDPDC`** command (see "Starting and stopping the data collector" on page 474).
2. If the DataPower data collector is registered as a service or daemon, deregister the service or daemon. For the procedure to stop a registered DataPower data collector, see "Running the DataPower data collector as a Windows service or UNIX daemon" on page 475. Deregister the service to remove it from the list of Windows services, if applicable.

WebSphere Message Broker:

Be sure to disable data collection for all brokers, execution groups, and message flows before upgrading your ITCAM for SOA installation to version 7.2.

You must also disable all WebSphere Message Broker data collectors when you upgrade WebSphere Message Broker from version 6.0 to version 6.1.3 or later. The user exit file name and directory structure for the data collector has changed since version 6.0. Disabling all data collection before performing these upgrades helps to ensure a smooth upgrade to the new structure.

Upgrading Tivoli Monitoring

Before you upgrade your ITCAM for SOA installation to version 7.2, you must upgrade your Tivoli Monitoring installation to the minimum supported version. The minimum supported version of Tivoli Monitoring for the ITCAM for SOA version 7.2 agent is available from the Software product compatibility reports website. For information about accessing reports on this website, see "Required software" on page 15.

This upgrade must be performed on each computer in your enterprise where these components of Tivoli Monitoring are installed:

- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

Each of these Tivoli Monitoring components must be upgraded before you upgrade to ITCAM for SOA version 7.2. Refer to your Tivoli Monitoring documentation for complete details about installing, upgrading, and configuring the Tivoli Monitoring environment.

Upgrading other monitoring agents:

Existing monitoring agents for other Tivoli products might also have to be upgraded. For information about upgrades, see your monitoring agent product documentation. Check whether upgrading to one of these supported versions of Tivoli Monitoring affects your existing monitoring agents.

Be sure to install or upgrade the following additional components of Tivoli Monitoring as needed:

- (Optional) Tivoli Enterprise Portal web browser enablement (also referred to as the *browser client*)
- Warehouse Proxy (if you intend to use historical reporting or save historical data to a database for later retrieval and analysis with the IBM Web Services Navigator, or for displaying historical data in certain ITCAM for SOA workspaces and views)
- IBM Eclipse Help Server, which is used to display searchable online help information in the IBM Eclipse Help System environment.
- The IBM Java Runtime Environment (JRE) or the Sun JRE for running the desktop version of the Tivoli Enterprise Portal
- Internet Explorer, with the Java plug-in (at the same version as the JRE) for running the web browser version of the Tivoli Enterprise Portal.

The procedures for installing and upgrading the additional Tivoli Monitoring are documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Roadmap for upgrading from ITCAM for SOA version 7.1.1 to version 7.2

You must upgrade ITCAM for SOA 7.1.1 (all releases) to version 7.2 before you update to ITCAM for SOA version 7.2 Fix Pack 1. To upgrade to version 7.2, complete the following tasks:

Table 5. Roadmap for upgrading to ITCAM for SOA version 7.2

Steps	Description
Install ITCAM for SOA version 7.2 application support files for the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal components of Tivoli Monitoring.	For more information, see “Enabling application support on the monitoring server, portal server, and desktop client” on page 36 on Windows systems or “Enabling application support on the monitoring server, portal server, and desktop client” on page 77 on Linux or UNIX systems.
Upgrade the existing ITCAM for SOA version 7.1.1 monitoring agents to version 7.2.	This upgrades the monitoring agents to version 7.2 and installs the ITCAM for SOA-specific data collectors for version 7.2. For information about updating the ITCAM for SOA monitoring agent, see the following sections: • “Installing and upgrading the ITCAM for SOA monitoring agent and data collectors” on page 40 on Windows systems • “Installing, upgrading, or updating the monitoring agent” on page 84 on Linux or UNIX systems
Exit the Data Collector Configuration Utility (ConfigDC).	When the ConfigDC utility starts, exit the utility. You can configure data collectors when you update to ITCAM for SOA version 7.2 Fix Pack 1.

Table 5. Roadmap for upgrading to ITCAM for SOA version 7.2 (continued)

Steps	Description
Upgrade topology support for Tivoli Common Object Repository and SOA Domain Management Server.	In your previous ITCAM for SOA version 7.1.1 installation, if you configured Tivoli Common Object Repository and SOA Domain Management Server, you must upgrade this topology support with the SOA Domain Management Server Configuration utility: • For the steps to upgrade a previous configuration of Tivoli Common Object Repository and SOA Domain Management Server on Windows systems, see "Upgrading a version 7.1.1 topology configured locally" on page 140 and "Upgrading a previous topology configured remotely" on page 144. • For the steps to upgrade a previous configuration of Tivoli Common Object Repository and SOA Domain Management Server on Linux or UNIX systems, see "Upgrading a version 7.1.1 topology configured locally" on page 202 and "Upgrading or updating a previous topology configured remotely" on page 205 **Remember:** You do not have to re-create the databases that are used for topology support. When you run the SOA Domain Management Server Configuration utility, the databases are migrated to the database schema for ITCAM for SOA version 7.2.
Reconfigure the Tivoli Enterprise Portal Server.	For information about reconfiguring the Tivoli Enterprise Portal, see "Reconfiguring and restarting the Tivoli Enterprise Portal Server" on page 173.

After upgrading ITCAM for SOA

After completing your upgrade or update tasks, if you installed the ITCAM for SOA monitoring agent on a supported Windows operating system, check the agent installation log file for locked JAR files.

Checking for locked JAR files

After completing your upgrade or update tasks, if you installed the ITCAM for SOA monitoring agent on a supported Windows operating system, check the agent installation log file for locked JAR files.

The log file is located at `*ITM_home*\InstallITM\IBM Tivoli Composite Application Management*.log`. Look for a message similar to one of the following examples:

```
CheckLockedFiles - File C:\IBM\ITM\TMAITM6\KD4\lib\kd4dcagent.jar is locked.
CheckLockedFiles - File C:\IBM\ITM\TMAITM6\KD4\lib\kd4dpdcagent.jar is locked.
```

If you see a locked file message for either of the listed JAR files, your data collector JAR files were not upgraded. If `kd4dcagent.jar` is locked, you did not disable the data collector from your BEA WebLogic Server. If the `kd4dpdcagent.jar` is locked, you did not stop the DataPower data collector before the upgrade. Contact IBM Support for assistance in obtaining the JAR files for the upgraded version of ITCAM for SOA.

Similarly, if you see a message that states that the `kd4ui.jar` file is locked, the ITCAM for SOA application client support for the desktop client was not upgraded because the desktop client was not stopped before the upgrade.

To unlock the JAR file, complete these steps:

1. Contact your Tivoli Enterprise Portal Server administrator and request a copy of the `kd4ui.jar` file.
   - On Windows system, the file is in the *ITM_home*`\CNB\classes` directory.

- On Linux and UNIX systems, the file is in the *ITM_home*/*platform*/cw/classes directory.

2. Copy the kd4ui.jar file to the *ITM_home*\CNP directory for your desktop client.
3. Then, reconfigure your desktop client to pick up the updated JAR file.

Updating to ITCAM for SOA version 7.2.0.1

This chapter describes the general procedures and considerations for updating the maintenance level of ITCAM for SOA from version 7.2 to version 7.2.0.1.

You do not have to update all of your ITCAM for SOA version 7.2 monitoring agents at the same time. During the time period when there is a mixture of version 7.1.1, version 7.2 and version 7.2.0.1 agents in your environment, the agents are supported at their respective levels of function.

When you update ITCAM for SOA monitoring agents to version 7.2.0.1, each of the existing runtime environments for the ITCAM for SOA data collectors on that computer must be upgraded to version 7.2.0.1.

Installing or migrating the WebSphere Application Server data collector

A new data collector, ITCAM Data Collector for WebSphere, was introduced in ITCAM for SOA version 7.2 for monitoring WebSphere Application Servers. ITCAM Data Collector for WebSphere is a shared component between the following components and products:

- ITCAM for SOA
- ITCAM Agent for WebSphere Applications
- ITCAM for WebSphere Application Server
- ITCAM for Transactions
- IBM Application Performance Diagnostics Lite

If ITCAM Data Collector for WebSphere is not installed, you install the data collector after you update the monitoring agent to version 7.2.0.1. You enable data collection for ITCAM for SOA using the ITCAM Data Collector for WebSphere Configuration utility in console mode or silent mode.

If an earlier version of ITCAM Data Collector for WebSphere is already installed, the installation of the data collector is skipped. However, after you update the monitoring agent to version 7.2.0.1, you must migrate the data collector. You migrate the data collector to the latest maintenance level using the ITCAM Data Collector for WebSphere Migration utility.

The procedure for installing the ITCAM Data Collector for WebSphere in the update roadmap assumes that neither the same nor an older version of the data collector is configured by another product for application servers in the same WebSphere profile. For the steps to complete when the same or an older version of the data collector is already configured, see “Installing ITCAM for SOA 7.2, updating to 7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere” on page 261.

The procedure for migrating the ITCAM Data Collector for WebSphere in the update roadmap assumes that neither the same nor an older version of the data collector is configured by another product for application servers in the same

WebSphere profile. For the steps to complete when the same or an older version of the data collector is already configured, see "Upgrading to V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere" on page 266.

If you plan to monitor business process applications through ITCAM for SOA, there are a number of options you must configure when installing and configuring IBM Business Process Manager. Before you update to ITCAM for SOA version 7.2.0.1, review the guidelines on installing and configuring IBM Business Process Manager in "Business Process Monitoring" on page 258.

Upgrading ITCAM for SOA on a Solaris platform

As Oracle supports only a clean installation on Solaris 11, you cannot update from ITCAM for SOA version 7.2 on Solaris 10 to ITCAM for SOA version 7.2.0.1 on Solaris 11. Instead, on a system where Solaris 10 and ITCAM for SOA version 7.2 are installed, complete these steps:

1. Create a backup of all of your data. Include any database files in your backup.
2. Perform a pristine installation of Solaris 11 on your system.
3. Restore your ITCAM for SOA version 7.2 configuration data on Solaris 11.
4. Update from ITCAM for SOA version 7.2 to version 7.2.0.1.

Before updating to ITCAM for SOA version 7.2 Fix Pack 1

Before you update ITCAM for SOA, complete the following tasks:

1. Close the Manage Tivoli Enterprise Monitoring Services utility if it is open on the application server where you are installing the monitoring agent.
2. Stop all application servers on the computer where the monitoring agent is being installed.

   Tip:

   - If you have the Microsoft .Net application server environment running on this application server, stop the `w3svc` service.
   - You do not have to stop the WebSphere Application Server or the WebSphere Message Broker environments if you use the migration scripts that are provided to migrate their data collectors.

   For information about stopping the current version of your application servers, see your product documentation.
3. Disable (unconfigure) any existing ITCAM for SOA data collectors on this computer system that are currently at version 7.2 and that you plan to upgrade to version 7.2 Fix Pack 1 (see "Disabling data collection for your monitoring environments" on page 25).
   You can use either the Data Collector Configuration utility (`ConfigDC`) or the `KD4ConfigDC` script to disable the ITCAM for SOA data collectors.

   Important:

   - You do not have to disable data collection for WebSphere Message Broker environments prior to the update. Instead, when you enable data collection, you are prompted to migrate any older versions of the data collector using an `upgradeBrokers` script (see "Upgrading to the Data Collector for WebSphere Message Broker" on page 360).
   - You do not have to unconfigure ITCAM Data Collector for WebSphere prior to the update. Instead, after you install the latest version of the data collector,

use the ITCAM Data Collector for WebSphere Migration utility to migrate the data collector configuration to the latest maintenance version.

For more information about updating the maintenance level of ITCAM Data Collector for WebSphere, see "Updating to V7.2 Fix Pack 1 and configuring ITCAM Data Collector for WebSphere" on page 272.

Disabling data collection for your monitoring environments

Before you update your current ITCAM for SOA installation, be sure to disable (unconfigure) data collection for all runtime environments. You can re-enable data collection for your runtime environments after the upgrade is complete.

DataPower environments:

Do not use the `–disable` option of the `KD4configDC` script or the Data Collector Configuration utility. Instead, you must complete the following steps:

1. Stop the DataPower data collector with the **`stopDC`** command (see "Starting and stopping the data collector" on page 474).
2. If the DataPower data collector is registered as a service or daemon, deregister the service or daemon. For the procedure to stop a registered DataPower data collector, see "Running the DataPower data collector as a Windows service or UNIX daemon" on page 475. Deregister the service to remove it from the list of Windows services, if applicable.

WebSphere Message Broker:

You do not have to disable data collection for WebSphere Message Broker environments prior to the update to version 7.2 Fix Pack 1. Instead, when you enable data collection, you are prompted to migrate any older versions of the data collector using an `upgradeBrokers` script (see "Upgrading to the Data Collector for WebSphere Message Broker" on page 360).

Roadmap for updating from ITCAM for SOA version 7.2 to version 7.2.0.1

After you install or upgrade to ITCAM for SOA version 7.2, you must update the agent to ITCAM for SOA version 7.2.0.1.

Before you update ITCAM for SOA, make sure you perform the prerequisite steps in "Before updating to ITCAM for SOA version 7.2 Fix Pack 1" on page 29.

To update to ITCAM for SOA version 7.2.0.1, complete the steps in Table 6.

Table 6. Roadmap for updating to ITCAM for SOA version 7.2.0.1

Steps	Description
Verify that ITCAM for SOA version 7.2 is installed.	To verify that ITCAM for SOA version 7.2 is installed, on Linux or UNIX systems issue the **`cinfo -d`** to display the list of Tivoli Monitoring components and agents. On Windows systems, issue the **`kincinfo -d`** command. The product code for ITCAM for SOA is d4. The version number for 7.2 is `07200000`. For example: `"d4","IBM Tivoli Composite Application Manager for SOA","aix523","07200000","100"` For information about the **`cinfo`** and the **`kincinfo`** commands, see the IBM Tivoli Monitoring Command Reference Guide in the ITCAM for Applications information center.

Table 6. Roadmap for updating to ITCAM for SOA version 7.2.0.1 (continued)

Steps	Description
Stop the ITCAM for SOA monitoring agent.	If the monitoring agent is started, stop it. For information about stopping the agent, see "Starting and stopping the monitoring agent" on page 513.
Enable application support for ITCAM for SOA version 7.2.0.1.	For more information, see "Enabling application support on the monitoring server, portal server, and desktop client" on page 36 on Windows systems or "Enabling application support on the monitoring server, portal server, and desktop client" on page 77 on Linux or UNIX systems.
Update the ITCAM for SOA to version 7.2.0.1.	Run the installation program to update the ITCAM for SOA agent to version 7.2.0.1. For information about using the installation program to update the monitoring agent, see "Installing and upgrading the ITCAM for SOA monitoring agent and data collectors" on page 40 on Windows systems and "Installing, upgrading, and updating the monitoring agents and data collectors" on page 81 on Linux and UNIX. Alternatively, you can remotely deploy the ITCAM for SOA agent using the **tacmd updateAgent** command. For information about remote deployment, see "Configuring for remote deployment of the monitoring agent" on page 63 on Windows systems and "Configuring for remote deployment of the monitoring agent" on page 97 on Linux and UNIX systems.
To configure data collection for a WebSphere Application Server, install or migrate to the ITCAM Data Collector for WebSphere.	To install ITCAM Data Collector for WebSphere and configure data collection, see "Step 18: Install ITCAM Data Collector for WebSphere" on page 55 on Windows systems and "Installing, upgrading, or updating the monitoring agent" on page 84 on Linux and UNIX systems. If the ITCAM Data Collector for WebSphere is already installed, you must migrate the data collector to the latest maintenance level. Data collection for the application server instances is enabled as part of the migration. For information about migrating the data collector, see "Updating to V7.2 Fix Pack 1 and configuring ITCAM Data Collector for WebSphere" on page 272.
Update the SOA Domain Management Server and the Tivoli Common Object Repository.	Run the ConfigDMS utility to update the SOA Domain Management Server and Tivoli Common Object Repository to 7.2.0.1. **Remember:** • You must configure topology support for ITCAM for SOA version 7.2 before you configure topology support for ITCAM for SOA version 7.2.0.1. • You do not have to re-create an existing SOA Domain Management Server database or Tivoli Common Object Repository database (local or remote). When you run the ConfigDMS utility, the databases are migrated to the database schema for ITCAM for SOA version 7.2.0.1. For information about running the ConfigDMS utility to upgrade the SOA Domain Management Server and Tivoli Common Object Repository, see Chapter 4, "Configuring topology support on Windows systems," on page 111 on Windows systems or Chapter 5, "Configuring topology support on Linux systems," on page 175 on Linux and UNIX systems.
Reconfigure the Tivoli Enterprise Portal Server.	For information about reconfiguring the Tivoli Enterprise Portal Server, see "Reconfiguring and restarting the Tivoli Enterprise Portal Server" on page 173 on Windows systems or "Rebuilding and restarting the Tivoli Enterprise Portal Server" on page 227 on Linux and UNIX systems.

Table 6. Roadmap for updating to ITCAM for SOA version 7.2.0.1 (continued)

Steps	Description
If you plan to send business process monitoring data to SmartCloud Application Performance Management UI, install and configure the ITCAM for SOA SDMS agent and its application support files.	For information about installing the agent, see Chapter 6, "Installing the ITCAM for SOA SDMS agent," on page 229.
Start the ITCAM for SOA monitoring agent.	For information about starting the agent, see "Starting and stopping the monitoring agent" on page 513.
Start the ITCAM for SOA SDMS monitoring agent, if installed.	For information about starting the agent, see "Starting and stopping the monitoring agent" on page 513.
Enable ITCAM for SOA-specific data collectors.	Enable data collection for runtime environments, as required. For information about enabling data collection, see the following sections: • For BEA WebLogic Server, see Chapter 12, "Configuring data collection: BEA WebLogic Server," on page 399. • For JBoss, see Chapter 13, "Configuring data collection: JBoss," on page 409. • For CICS Transaction Server, see Chapter 14, "Configuring data collection: CICS Transaction Server," on page 415. • For SAP NetWeaver, see Chapter 15, "Configuring data collection: SAP NetWeaver," on page 417. • For WebSphere Community Edition, see Chapter 16, "Configuring data collection: WebSphere Community Edition," on page 431. • For DataPower SOA Appliance, see Chapter 17, "Configuring data collection: DataPower SOA Appliance," on page 441.
Enable Data Collector for WebSphere Message Broker.	Enable data collection for WebSphere Message Broker environments, if required. For more information about enabling data collection, see Chapter 9, "Configuring data collection: WebSphere Message Broker," on page 359.
Integrate DataPower SOA appliance and Microsoft .NET data collectors with ITCAM for Transactions.	(Optional) Integrate the DataPower SOA appliance and Microsoft .NET data collectors with ITCAM for Transactions. For information about integrating the data collectors with ITCAM for Transactions, see Chapter 18, "Integrating with ITCAM for Transactions," on page 489.
Enable historical data collection.	(Optional) Enable data collection for ITCAM for SOA. If you configured historical data collection for ITCAM for SOA version 7.1.1 or 7.2, review the attribute groups that are configured for data collection. A specific set of attribute groups must be enabled for data collection to view data in ITCAM for SOA workspaces, Web Services Navigator, and ITCAM for SOA Reports. **Important:** After you update to version 7.2.0.1, data is not viewable in the Tivoli Enterprise Portal until one of the following conditions occurs: • The Warehouse Proxy Agent exports its first batch of data for a specific attribute group. • The Summarization and Pruning agent runs for the first time after the upgrade to ITCAM for SOA version 7.2.0.1. For information about enabling historical data collection, see Chapter 19, "Enabling historical data collection," on page 497.

Table 6. Roadmap for updating to ITCAM for SOA version 7.2.0.1 (continued)

Steps	Description
Install the latest version of the Discovery Library Adapters (DLAs) that are provided with ITCAM for SOA.	(Optional) Install the DLAs that populate the Tivoli Common Object Repository database with relationship information to display in Tivoli Enterprise Portal topology workspaces and views. The same versions of the DLAs are provided in ITCAM for SOA 7.2 and ITCAM for SOA 7.1.1. However, an additional WebSphere Service Registry and Repository DLA is provided in ITCAM for SOA version 7.2. If you want to discover services in WebSphere Service Registry and Repository version 8.0, you must install the WebSphere Service Registry and Repository DLA using the `WSRR8_DLA.bat` script. If you want to discover services in WebSphere Service Registry and Repository version 8.5, you must update to ITCAM for SOA version 7.2 Fix Pack 1 Interim Fix 2 (7.2.0.1 IF2) or later and then install the WebSphere Service Registry and Repository DLA using the `WSRR85_DLA.bat` script. The same versions of the DLAs are provided in ITCAM for SOA 7.2.0.1 and ITCAM for SOA 7.2.
Install the latest version of ITCAM for SOA Tools.	(Optional) Install ITCAM for SOA Tools, which includes the Web Services Navigator. If you installed ITCAM for SOA Tools as part of ITCAM for SOA versions 7.1.1 or 7.2, you must uninstall the previous version of ITCAM for SOA Tools before you install the version that is provided with ITCAM for SOA version 7.2.0.1. To view data from Tivoli Data Warehouse in the Web Services Navigator, establish a connection to one or more supported databases where historical metric data is being stored. For information about uninstalling and installing ITCAM for SOA Tools, see the *IBM Tivoli Composite Application Manager for SOA Tools* guide.
Import ITCAM for SOA reports into Tivoli Common Reporting.	(Optional) Import ITCAM for SOA reports into Tivoli Common Reporting. If you installed ITCAM for SOA Reports as part of ITCAM for SOA version 7.2, you must install the version that is provided with ITCAM for SOA version 7.2.0.1. ITCAM for SOA Reports metadata relating to the Fault Log attribute group changed in version 7.2.0.1.For information about installing ITCAM for Reports, see the *IBM Tivoli Composite Application Manager for SOA Reports Guide*.
Configure Tivoli Monitoring to forward ITCAM for SOA events.	(Optional) Configure Tivoli Monitoring to forward events from ITCAM for SOA to an external destination. For information about forwarding events, see Chapter 23, “Configuring Tivoli Monitoring to forward events,” on page 509.

Table 6. Roadmap for updating to ITCAM for SOA version 7.2.0.1 (continued)

Steps	**Description**
Integrate ITCAM for SOA events with WebSphere Service Registry and Repository.	(Optional) Integrate ITCAM for SOA events with WebSphere Service Registry and Repository. Configure forwarding of ITCAM for SOA situations events to WebSphere Service Registry and Repository. If you integrated ITCAM for SOA with WebSphere Service Registry and Repository before you updated to version 7.2 fix pack 1, you must deploy the WSRR SDMS configuration file again. If you plan to integrate with WebSphere Service Registry and Repository 8.0 for the first time, there are additional settings that you have to configure. A separate WSRR SDMS configuration template is provided for version 8.0. For more information about configuring the interface between ITCAM for SOA and WebSphere Service Registry and Repository, see *IBM Tivoli Composite Application Manager for SOA WSRR Integration Guide*.
Verify that ITCAM for SOA agent is correctly installed.	For information about verifying the installation of ITCAM for SOA, see Chapter 24, "Verifying the installation and configuration," on page 511.

Chapter 2. Installing or upgrading ITCAM for SOA on Windows systems

Before you install ITCAM for SOA version 7.2 Fix Pack 1, refer to "Performing a pristine installation of ITCAM for SOA version 7.2 Fix Pack 1" on page 19 for the ITCAM for SOA installation prerequisites and for the roadmap of installation tasks.

Before you upgrade to ITCAM for SOA version 7.2, refer to "Upgrading to ITCAM for SOA version 7.2" on page 23 for the ITCAM for SOA upgrade prerequisites and for the roadmap of upgrade tasks.

Before you update to ITCAM for SOA version 7.2 Fix Pack 1, refer to "Updating to ITCAM for SOA version 7.2.0.1" on page 28 for the ITCAM for SOA update prerequisites and for the roadmap of update tasks.

Remember: ITCAM for SOA supports only a single installation per computer system.

Permissions for installing, upgrading, or updating the monitoring agent

To install, upgrade, or update the monitoring agent, you must have the following permissions:

- You must have administrator privileges on the computer system where the monitoring agent is being installed.
- You must run the monitoring agent as a user with administrator privileges.
- All IBM Tivoli Monitoring components, including the monitoring agent, must be installed and run as the same user. For more information about permissions, see the User Authority section of the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing ITCAM for SOA on a 64-bit system

If you are installing or upgrading ITCAM for SOA on a Windows 64-bit system, if a 64-bit agent is installed, you must install the 32/64 Bit Agent Compatibility Package and the agent framework for x86-64 bit environments.

In ITCAM for SOA version 7.2, the agent compatability package is not bundled with the agent. Instead, you must install the agent compatability package that is provided with Tivoli Monitoring version 6.2.3 before you install the ITCAM for SOA agent. Tivoli Monitoring is provided with ITCAM for Applications version 7.2 and Application Performance Management version 7.6. To install the agent compatibility package, complete the following steps:

- Locate the installation media for IBM Tivoli Monitoring version 6.2.3.
- From the `WINDOWS` subdirectory of the Tivoli Monitoring installation media, run `setup.exe`. The installation wizard starts.
- On the Select Features page, leave all of the existing check boxes selected. The following two components are selected by default:
  - 32/64 Bit Agent Compatibility Package (x86-64 only)
  - Tivoli Enterprise Monitoring Agent Framework (x86-64 only)

- Follow the instructions on the Tivoli Monitoring installation wizard to complete the installation of the agent compatibility package.
- Run the ITCAM for SOA installation wizard to complete the installation of ITCAM for SOA.

Important: You can install the agent compatibility package from any media where it is bundled, but the version that is installed must be greater than or equal to V6.2.2 Fix Pack 3.

If you are upgrading to ITCAM for SOA 7.2 Fix Pack 1 on a Windows 64-bit system, after you select the ITCAM for SOA agent in the installation wizard, both features are selected automatically if the following conditions are met:

- You are installing on a 64-bit system.
- Another 64-bit agent is installed on the system.
- The 32/64 Bit Agent Compatibility Package is not already installed.

Enabling application support on the monitoring server, portal server, and desktop client

To ensure the monitoring agent works within your Tivoli Monitoring infrastructure, application support files must be distributed to the Tivoli Monitoring components.

Application support files are provided with the installation of the ITCAM for SOA agent.

Application support files are automatically installed and enabled on the monitoring server without the need to recycle the monitoring server if you are integrating with Tivoli Monitoring version 6.2.3 or later and the Tivoli Monitoring components and the agent are enabled for self-description. The conditions that must be met for self-description to operate are specified in “Enabling application support through self-description.” Application support files must be manually installed on the portal server and the portal client.

If the agent and the Tivoli Monitoring components are not enabled for self-description, you must manually install application support files on the Tivoli Monitoring components. For more information, see “Installing and enabling application support manually before installing the agent” on page 37.

Enabling application support through self-description

Tivoli Monitoring version 6.2.3 or later agents, which are enabled for self-description, install application support files and enable application support on the IBM Tivoli Monitoring infrastructure automatically.

ITCAM for SOA is enabled by default for self-description. When the ITCAM for SOA agent is installed and the hub and remote monitoring servers are enabled for self-description, application support files are automatically installed on the hub monitoring server and the remote monitoring server, without the need to recycle the monitoring server.

Application support files must be installed manually on portal server and the portal client. ITCAM for SOA requires that configuration of topology support for SOA Domain Management Server and Tivoli Common Object Repository on the portal server be performed manually.

Although the self-describing agent is enabled by default for ITCAM for SOA, a number of conditions apply:

- All Tivoli Management Services server components must be at version 6.2.3 or later.
- The agent framework must be at version 6.2.3 or later.

In ITCAM for SOA version 7.2 and later, agent framework version 6.2.2 is installed a part of an install or upgrade of ITCAM for SOA. Install Tivoli Monitoring version 6.2.3 OS agent and framework to update the framework to version 6.2.3.

Remember: Not all OS agents running version 6.2.3, which share the same IBM Tivoli Monitoring home directory as ITCAM for SOA, upgrade the agent framework to version 6.2.3. You must verify that the agent framework has been upgraded to version 6.2.3 before using self-description for ITCAM for SOA.

To identify the agent framework version after installing or upgrading ITCAM for SOA, complete the following steps:

1. From the command prompt, navigate to *ITM_home*\bin directory.
2. Run the following command:
   ```
   Kincinfo -t
   ```
3. Locate the line for the agent framework in the output and note the version. For example:
   ```
   PC    PRODUCT        DESC      PLAT      VER          BUILD     INSTALL DATE
   GL  Tivoli Enterprise Monitoring Agent Framework   WIX64  06.23.02.00
   d2215a
    20120816 1412
   ```

You must verify that these conditions are met before you can use self-description for deploying application support to the monitoring server.

When the self-describing application update is complete, and the application support files are manually installed on the portal server, you should see the following new agent data in the portal client:

- Historical Configuration is updated with any new attributes
- Workspaces are updated
- New or updated situations, policies and take actions
- Queries are updated
- Help server files are updated

The self-describing agent feature is disabled by default on the hub monitoring server. The procedure for enabling self-description on the hub monitoring server is documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing and enabling application support manually before installing the agent

Enabling application support is sometimes referred to as adding or activating application support.

Multiple versions of ITCAM for SOA can be integrated with Tivoli Monitoring. If self-description is not enabled, you must install application support files from the agent that is at the latest version. For example, if your environment has ITCAM for SOA versions 7.2 and 7.1.1, ensure you install the application support files for the latest version, in this case version 7.2.

You must stop the monitoring server, portal server, or portal client when installing the support files.

The following procedures refer to adding application support when the Tivoli Monitoring components are installed on a separate computer system to the monitoring agent. If the ITCAM for SOA monitoring agent and the Tivoli Monitoring components are on the same computer system, application support files are installed as part of the monitoring agent installation.

When all of the Tivoli Monitoring components are installed on the same computer system, application support files for each of the monitoring components must be installed at the same time.

When you manually install application support on your Tivoli Enterprise Monitoring Server, you must be logged in as the user who installed the Tivoli Enterprise Monitoring Server.

The Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal must be stopped before you install the application support files. To stop Tivoli Monitoring components, complete the following steps:

1. Launch Manage Tivoli Enterprise Monitoring Services.
2. Right-click the component that you want to stop.
3. Click **Stop** from the menu.

Complete the following steps to manually install application support for the ITCAM for SOA agent on a single computer:

1. When you load the ITCAM for SOA installation media, locate and double-click the `setup.exe` file within the WINDOWS directory.
2. On the Welcome page, click **Next**.
3. The Software License Agreement page is displayed. Accept the license agreement and click **Next**.
4. From the Select Features page, select **Tivoli Enterprise Monitoring Server - TEMS**, **Tivoli Enterprise Portal Server - TEPS**, and **TEP Desktop client -TEPD** and click **Next**.
5. The Agent Deployment page provides an option to install the Tivoli Enterprise Monitoring Agent remotely. Click **Next** without selecting the **IBM Tivoli Composite Application Manager for SOA**, or the **Tivoli Enterprise Services user Interface Extensions** check boxes.
   For more information about remote deployment of the monitoring agent, see "Configuring for remote deployment of the monitoring agent" on page 63.
6. Review the installation summary details and click **Next** to start the installation.
   The application support packages for the monitoring server, portal server, and portal desktop client are installed.
7. On the Setup Type window, complete the following steps:
   a. Select the **Install application support for a local/remote Tivoli Enterprise Monitoring Server** check box.
   b. (Optional) Select the check box for starting the Manage Tivoli Enterprise Monitoring Servers window. (If selected, this window is displayed when the installation procedure is finished.)
   c. (Optional) Select the check box for configuring the default connection from the monitoring agent to the Tivoli Enterprise Monitoring Server.

The option for configuring the Tivoli Enterprise Portal is mandatory (preceded by an asterisk [*]) and cannot be cleared.
Click **Next**.

8. The TEPS Hostname window is displayed. The host name for the local computer is displayed. Accept the default value and click **Next**.
9. To activate application support on the monitoring server, specify the location of the monitoring server. In the **Add application support to the TEMS** window, select **On this computer** and click **OK**.
10. Select the application support component that you want to add to the monitoring server and click **OK**.
By default, the application support for IBM Tivoli Composite Application Manager for SOA is already selected.
11. Click **Next** on the message that provides the results of the process of adding application support.
12. If you selected the option to configure the default connection from the monitoring agent to the monitoring server in step 7 on page 38, the Configuration Defaults for Connecting to a TEMS window is displayed. For information about configuring the connection to the monitoring server, see "Configuring the monitoring agent" on page 58.
13. The InstallShield Wizard Complete page is displayed indicating that the installation was successful, and providing an option to view the readme file for the product. Click **Finish**.
14. If you selected the **Launch Manage Tivoli Monitoring Services** check box in 7 on page 38, the Manage Tivoli Enterprise Monitoring Services utility opens.
15. Restart Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal. Complete these steps:
    a. Launch Manage Tivoli Enterprise Monitoring Services.
    b. Right-click the component that you want to start.
    c. Click **Start** from the menu.

Verifying User Account Control settings on Windows 7 platform

On Windows 7 platforms, the User Account Control (UAC) setting is set to level 3, `Notify me only when programs try to make changes to my computer`, by default. Level 3 is the recommended setting for installing ITCAM for SOA in interactive and silent mode on a local system. All other settings are restrictive.

To verify that the value of the UAC setting is set to level 3, go to **Start** -> **Control Panel** -> **Action Center** -> **Change User Account Control Settings**.

The ITCAM for SOA installer must be run as the administrator to ensure that sufficient permissions are granted before the installation begins. To run the installer as the administrator, right-click the `setup.exe` file in the file explorer and choose **Run as Administrator**.

Important: Remote deployment of ITCAM for SOA on a remote Windows 7 platform is not supported.

Installing and upgrading the ITCAM for SOA monitoring agent and data collectors

Use the installation wizard to install, upgrade, or update the agent on each computer system where one or more of the supported application server runtime environments (for example, WebSphere Application Server) are installed. For a DataPower environment, install the agent on the computer system where the DataPower proxy is located.

- In the installation wizard, if you are upgrading to ITCAM for SOA version 7.2, the ITCAM for SOA monitoring agent is displayed as `IBM Tivoli Composite Application Manager for SOA  V07.20.00.00`.
- If you are installing or updating to ITCAM for SOA version 7.2 Fix Pack 1, the ITCAM for SOA monitoring agent is displayed as `IBM Tivoli Composite Application Manager for SOA  V07.20.01.00`.

Installing the monitoring agent and the data collectors

The agent consists of the monitoring agent and the data collector components. A data collector intercepts request and response messages of the services that you are monitoring. The monitoring agent collects the information from the data collector, and transfers the information to the monitoring server for presentation and storage. In ITCAM for SOA version 7.2, there are two types of data collectors:

- ITCAM for SOA-specific data collectors, installed automatically as part of the installation of the monitoring agent and used to configure data collection for all runtime environments, apart from the WebSphere Application Server and WebSphere Message Broker environments.
- The ITCAM Data Collector for WebSphere, used to configure data collection for WebSphere application server instances

In ITCAM for SOA version 7.2 Fix Pack 1, the Data Collector for WebSphere Message Broker is introduced to configure data collection for WebSphere Message Broker environments

Before ITCAM for SOA version 7.2, both the data collector components and the monitoring agent component were installed or upgraded as part of the installation or upgrade of the monitoring agent. In ITCAM for SOA version 7.2 and later, the ITCAM Data Collector for WebSphere is installed after the monitoring agent is installed in a location that you specify.

After the monitoring agent installation completes, the installer automatically starts the Data Collector Configuration Utility for enabling data collection in the supported runtime environments. For all data collectors, apart from the ITCAM Data Collector for WebSphere, as soon as the Data Collector Configuration utility launches, the installation of the data collector is complete, and you can enable data collection with this utility. Alternatively, you can exit this utility and use the `KD4ConfigDC` script to configure the data collector.

Installing and configuring the ITCAM Data Collector for WebSphere

Beginning with ITCAM for SOA version 7.2, the ITCAM Data Collector for WebSphere is a new component that is shared with the following components and products:

- ITCAM for SOA

- ITCAM Agent for WebSphere Applications
- ITCAM for WebSphere Application Server
- IBM Application Performance Diagnostics Lite
- ITCAM for Transactions

Because this data collector component was not in version 7.1.1, when you are upgrading from version 7.1.1, you must install it in a location that you specify before you enable the data collector. The data collector must be configured using the new ITCAM Data Collector for WebSphere Configuration utility command-line utility.

When the installation, upgrade, or update of the monitoring agent completes, the `ConfigDC` utility is started. When you select the option to configure the WebSphere Application Server, a command-line window opens and you are prompted to specify the data collector home directory. Next, the data collector is installed in the specified directory. If the same version, release, and maintenance level of the data collector is already installed in the directory, the data collector is not reinstalled.

The ITCAM Data Collector for WebSphere Configuration utility for configuring the data collector is started in console mode. You must integrate the data collector with the ITCAM for SOA monitoring agent with this utility.

Considerations for the installation or upgrade of the monitoring agent and data collectors

This installation of the monitoring agent and data collectors is based on the following assumptions:

- You installed or upgraded your Tivoli Monitoring environment to one of the minimum supported levels (see “Software and hardware prerequisites” on page 15).
- As part of the process of installing or upgrading your Tivoli Monitoring environment, you installed and configured one or more supported database applications (IBM DB2, Microsoft SQL Server, or Oracle). The database application is used for storing historical data or for viewing service registry, business process, or service-to-service topology data in your Tivoli Monitoring workspaces. For database information, see “Databases” on page 13.
- You already installed or upgraded application support for the Tivoli Monitoring components. For more information about installing application support, see “Enabling application support on the monitoring server, portal server, and desktop client” on page 36. If your IBM Tivoli Monitoring components are installed on the same computer systems as your application server runtime environment, application support can be installed during the installation of the monitoring agent.

The appropriate level of the Tivoli Enterprise Management Agent Framework is installed when the monitoring agent is installed.

In IBM Tivoli Monitoring version 6.2.3, the `tacmd` commands moved to the new Tivoli Enterprise Services User interface Extensions component. The new user interface extensions are an optional installable component of the monitoring agent.

Run the installation program on the ITCAM for SOA installation media on a supported Windows operating system by completing the following steps for each computer (or, in the case of a DataPower environment, on the computer where the

DataPower proxy data collector is located) where you are installing the monitoring agent.

Step 1: Start setup.exe

When you load the ITCAM for SOA installation media, locate and double-click the `setup.exe` file within the `WINDOWS` directory. The installer starts and a Welcome page is displayed. Click **Next**.

Remember: On Windows 7 platforms, the ITCAM for SOA installer must be run as the administrator to ensure that sufficient permissions are granted before the installation or upgrade begins. Right-click the `setup.exe` file in the file explorer and click **Run as Administrator**.

The Software License Agreement window is displayed.

Step 2: Accept the software license agreement

Read and accept the software license agreement.

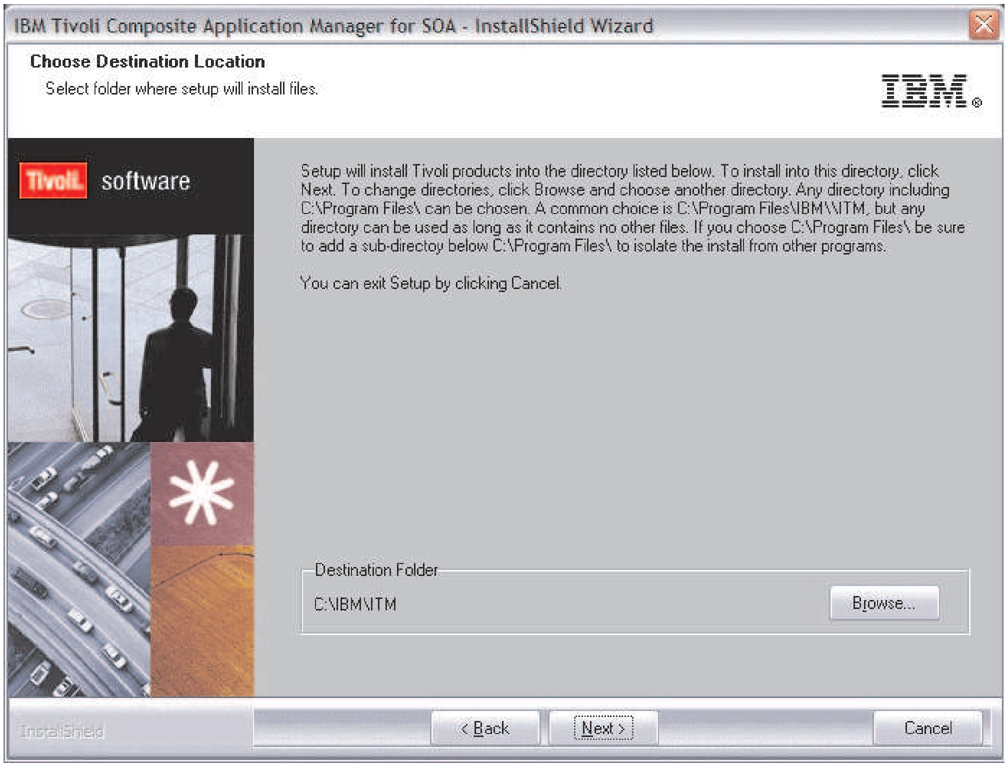
If you do not have a database (IBM DB2, Microsoft SQL Server, or Oracle) installed on this computer for temporarily storing data before forwarding the data to the monitoring server, a message is displayed indicating that software might be missing. However, you do not have to have a database installed to install the monitoring agent.

Click **Next**.

Step 3: Choose the destination folder for the installation files

In an upgrade or update installation, or if you installed IBM Tivoli Monitoring components on the same server, the destination directory is determined automatically and this step is skipped.

On a new installation, the **Choose destination location** window opens.



IBM Tivoli Composite Application Manager for SOA - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

Setup will install Tivoli products into the directory listed below. To install into this directory, click Next. To change directories, click Browse and choose another directory. Any directory including C:\Program Files\ can be chosen. A common choice is C:\Program Files\IBM\\ITM, but any directory can be used as long as it contains no other files. If you choose C:\Program Files\ be sure to add a sub-directoy below C:\Program Files\ to isolate the install from other programs.

You can exit Setup by clicking Cancel.

Destination Folder

C:\IBM\ITM

Figure 2. Choosing the destination installation directory.

This window shows the folder (*ITM_home*) where the agent is to be installed. The destination folder can be shared with other IBM Tivoli Monitoring products. To use a location other than the default (`C:\IBM\ITM`), click **Browse**, and select the folder that you want to use.

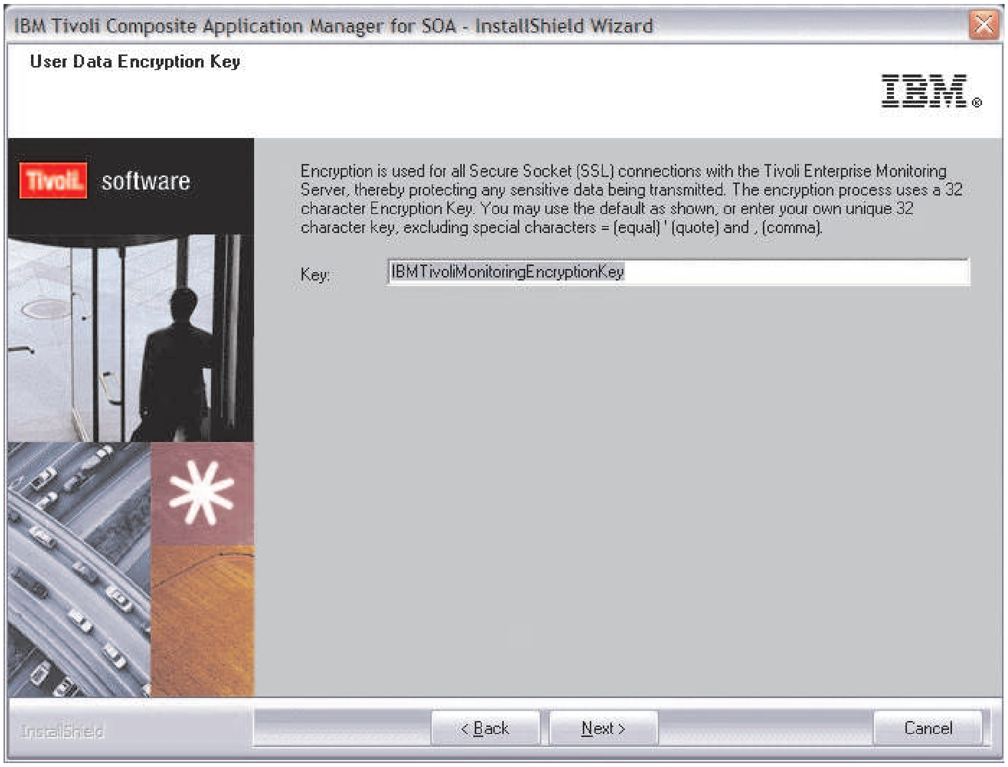
After the correct folder is specified, click **Next**.

Tip: If you are installing ITCAM for SOA over an existing installation, you might receive a message to remind you that there are newer versions of the Tivoli Monitoring components that can be installed. The message indicates that you can choose not to install the newer versions of each component in the following steps. The newer versions of the application support files might not work correctly with previous versions of the monitoring agents.

Step 4: Enter the IBM Tivoli Monitoring encryption key

In an upgrade or update of an installation, or when some IBM Tivoli Monitoring components are already installed, the data encryption key is already set, and this step is skipped.

On a new installation, the **User Data Encryption Key** page opens. It prompts you for the 32-character encryption key that is used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment:



IBM Tivoli Composite Application Manager for SOA - InstallShield Wizard

User Data Encryption Key

Encryption is used for all Secure Socket (SSL) connections with the Tivoli Enterprise Monitoring Server, thereby protecting any sensitive data being transmitted. The encryption process uses a 32 character Encryption Key. You may use the default as shown, or enter your own unique 32 character key, excluding special characters = (equal) ' (quote) and , (comma).

Key: IBMTivoliMonitoringEncryptionKey

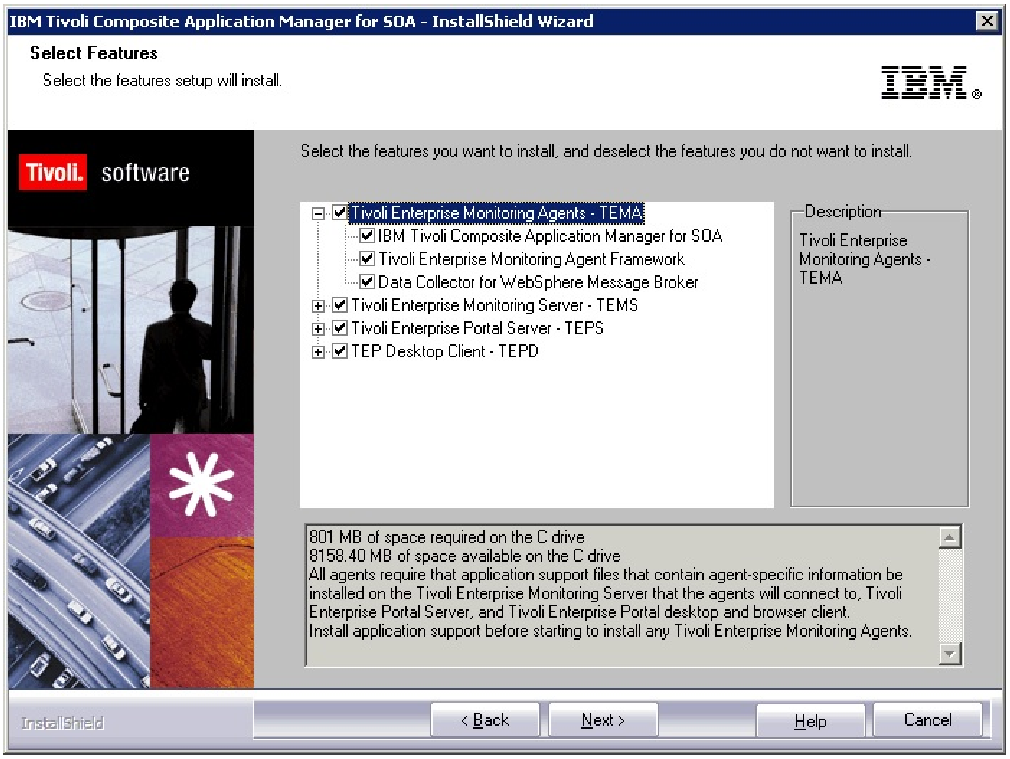
Figure 3. The User Data Encryption Key page

A default value, `IBMTivoliMonitoringEncryptionKey`, is displayed. Either accept the default value, or enter your own encryption key, and click **Next**.

Remember: The encryption key must be the same as the key that was used during the installation of the monitoring server to which the agent connects.

Step 5: Select the product components you want to install

The Select Features window is displayed.


IBM Tivoli Composite Application Manager for SOA - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

- ☑ Tivoli Enterprise Monitoring Agents - TEMA
  - ☑ IBM Tivoli Composite Application Manager for SOA
  - ☑ Tivoli Enterprise Monitoring Agent Framework
  - ☑ Data Collector for WebSphere Message Broker
- ☑ Tivoli Enterprise Monitoring Server - TEMS
- ☑ Tivoli Enterprise Portal Server - TEPS
- ☑ TEP Desktop Client - TEPD

Description

Tivoli Enterprise Monitoring Agents - TEMA

801 MB of space required on the C drive
8158.40 MB of space available on the C drive
All agents require that application support files that contain agent-specific information be installed on the Tivoli Enterprise Monitoring Server that the agents will connect to, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop and browser client.
Install application support before starting to install any Tivoli Enterprise Monitoring Agents.

Figure 4. The Select Features page, showing the expanded Tivoli Enterprise Monitoring Agent node.

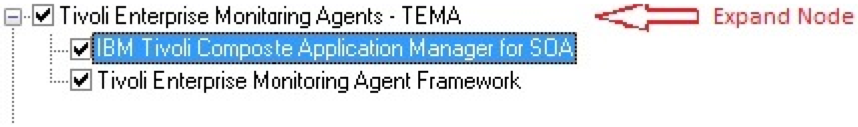
The features that are selected by default depend on whether you are installing IBM Tivoli Monitoring for the first time.

Select the **Tivoli Enterprise Monitoring Agents - TEMA** check box to expand this node, and select the **IBM Tivoli Composite Application Manager for SOA** and the **Tivoli Enterprise Monitoring Agent Framework** check boxes.

When installing or updating to ITCAM for SOA version 7.2 Fix Pack 1, if you plan to configure data collection for a WebSphere Message Broker environment, select the **Data Collector for WebSphere Message Broker** check box. Before you install the data collector, verify that the data collector is not already installed as part of ITCAM for Transactions.

- If the data collector is already installed as part of ITCAM for Transactions and is at the same maintenance level, skip the steps to install and enable the data collector. Instead, integrate the data collector with the ITCAM for SOA monitoring agent by setting the `default.kd4.enabled` property in the `KK3.dc.properites` file to `true`. For more information about integrating the data collector with ITCAM for SOA, see “Integrating the data collector with ITCAM for SOA and ITCAM for Transactions” on page 368.
- If the data collector is installed but is at an earlier maintenance level, install the data collector and follow the procedure for updating the maintenance level of the data collector in “Upgrading to the Data Collector for WebSphere Message Broker” on page 360.
- If an older version of the data collector is installed, follow the upgrade procedure in“Upgrading to the Data Collector for WebSphere Message Broker” on page 360.

Important: Make sure to expand the Tivoli Enterprise Monitoring Agents - TEMA node to explicitly verify that at least IBM Composite Tivoli Composite Application Manager for SOA and the Tivoli Enterprise Monitoring Agent Framework are checked as shown:



- ☑ Tivoli Enterprise Monitoring Agents - TEMA
  - ☑ IBM Tivoli Composte Application Manager for SOA
  - ☑ Tivoli Enterprise Monitoring Agent Framework

Expand Node

Select the following nodes also if you are installing application support files as part of the installation, update, or upgrade of ITCAM for SOA:

- Tivoli Enterprise Monitoring Server - TEMS
- Tivoli Enterprise Portal Server - TEPS
- TEP Desktop Client - TEP

If you are upgrading to ITCAM for SOA 7.2 Fix Pack 1 on a Windows 64-bit system, two additional features are available for selection:

- `32/64 Bit Agent Compatibility Package (x86-64 only)`
- `Tivoli Enterprise Monitoring Agent Framework (x86-64 only)`

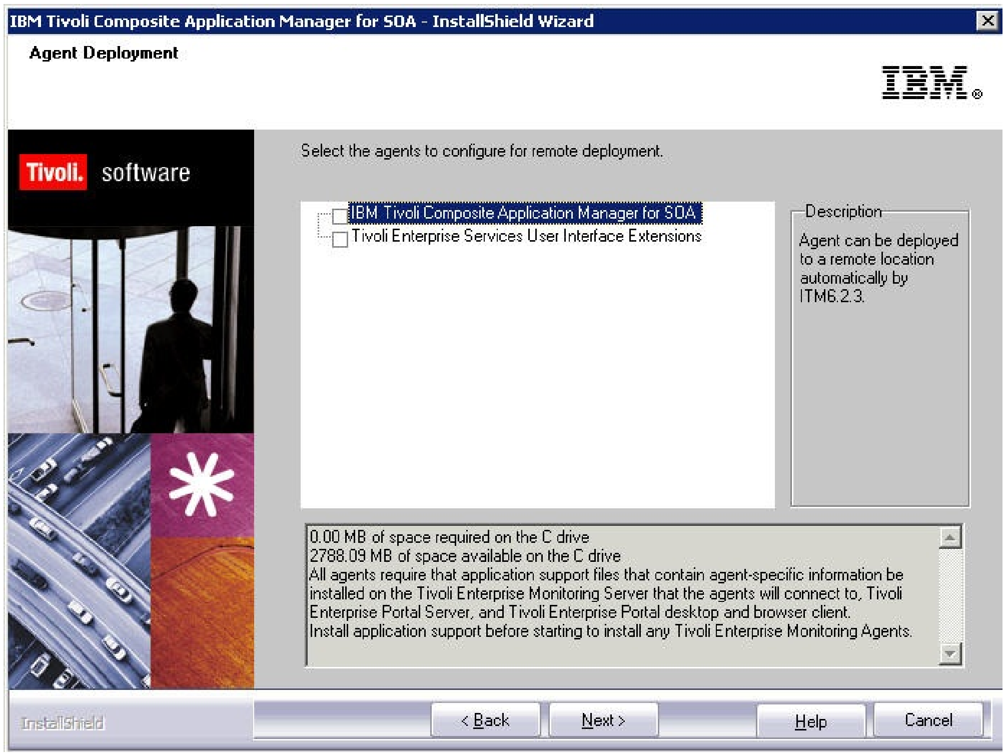
The Agent Compatibility Package provides support for installing 32-bit agents on a system where 64-bit agents are installed. The `32/64 Bit Agent Compatibility Package (x86-64 only)` and `Tivoli Enterprise Monitoring Agent Framework (x86-64 only)` options are automatically selected if the following conditions are met:

- You are installing on a 64-bit system.
- Another 64-bit agent is installed on the system.
- The 32/64 Bit Agent Compatibility Package is not already installed.

Click **Next**.

Step 6: View the option to remotely deploy monitoring agent

If you are installing the monitoring agent on a computer that already has a monitoring server installed, the Agent Deployment window is displayed. The Agent Deployment window provides an option to install the Tivoli Enterprise Monitoring Agent remotely.



IBM Tivoli Composite Application Manager for SOA - InstallShield Wizard
Agent Deployment
IBM
Tivoli. software
InstallShield
< Back
Next >
Help
Cancel

Select the agents to configure for remote deployment.

□ IBM Tivoli Composite Application Manager for SOA
□ Tivoli Enterprise Services User Interface Extensions

Description

Agent can be deployed to a remote location automatically by ITM6.2.3.

0.00 MB of space required on the C drive
2788.09 MB of space available on the C drive
All agents require that application support files that contain agent-specific information be installed on the Tivoli Enterprise Monitoring Server that the agents will connect to, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop and browser client.
Install application support before starting to install any Tivoli Enterprise Monitoring Agents.

Figure 5. The Agent Deployment page

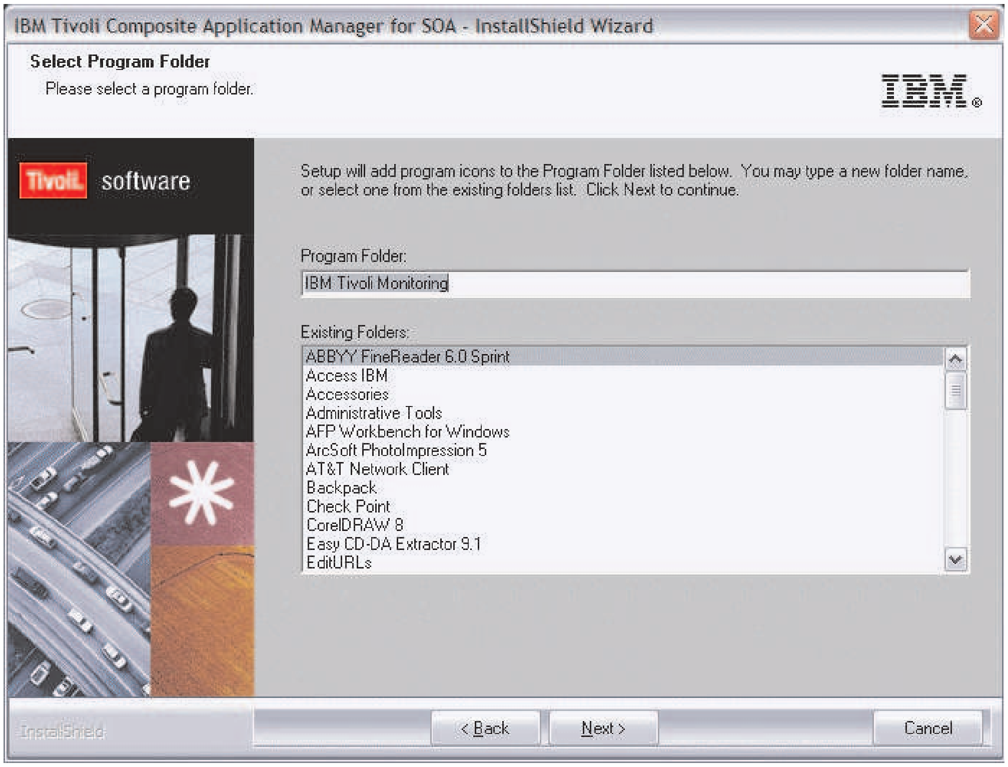
For more information about remote deployment of the monitoring agent, see "Configuring for remote deployment of the monitoring agent" on page 63.

Click **Next** without selecting **IBM Tivoli Composite Application Manager for SOA** or **Tivoli Enterprise Services User Interface Extensions**.

Step 7: Select a Windows program folder

In an upgrade or update of an installation, or when the current version of the Tivoli Enterprise Monitoring Agent is installed on the host, or when some IBM Tivoli Monitoring components are already installed, this step is skipped. The reinstallation uses the same program folder as the existing installation.

If you are performing a pristine installation on a computer system where no IBM Tivoli Monitoring components are installed, the Select Program Folder window opens. It displays the Windows program folder for programs:


IBM Tivoli Composite Application Manager for SOA - InstallShield Wizard
IBM
Tivoli software
InstallShield
< Back
Next >
Cancel

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folder: IBM Tivoli Monitoring

Existing Folders:

- ABBYY FineReader 6.0 Sprint
- Access IBM
- Accessories
- Administrative Tools
- AFP Workbench for Windows
- ArcSoft PhotoImpression 5
- AT&T Network Client
- Backpack
- Check Point
- CorelDRAW 8
- Easy CD-DA Extractor 9.1
- EditURLs

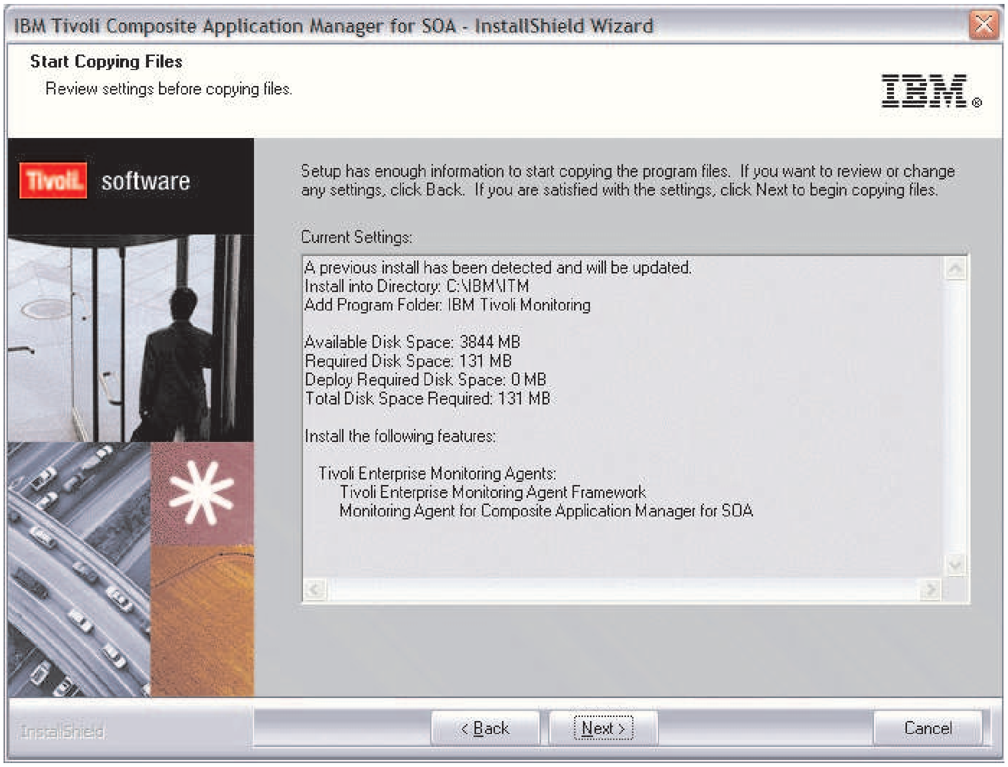
Figure 6. Specifying the program folder name

You can modify the name of the folder (under the **Programs** menu) where IBM Tivoli Monitoring programs are listed.

Click **Next**.

Step 8: Verify selected features

The Start Copying Files window opens, displaying the features that you selected, the disk space requirements for the installation, and the available disk space.


IBM Tivoli Composite Application Manager for SOA - InstallShield Wizard
Start Copying Files
Review settings before copying files.
IBM
Tivoli software
InstallShield
< Back
Next >
Cancel

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

A previous install has been detected and will be updated.
Install into Directory: C:\IBM\ITM
Add Program Folder: IBM Tivoli Monitoring

Available Disk Space: 3844 MB
Required Disk Space: 131 MB
Deploy Required Disk Space: 0 MB
Total Disk Space Required: 131 MB

Install the following features:

Tivoli Enterprise Monitoring Agents:
Tivoli Enterprise Monitoring Agent Framework
Monitoring Agent for Composite Application Manager for SOA

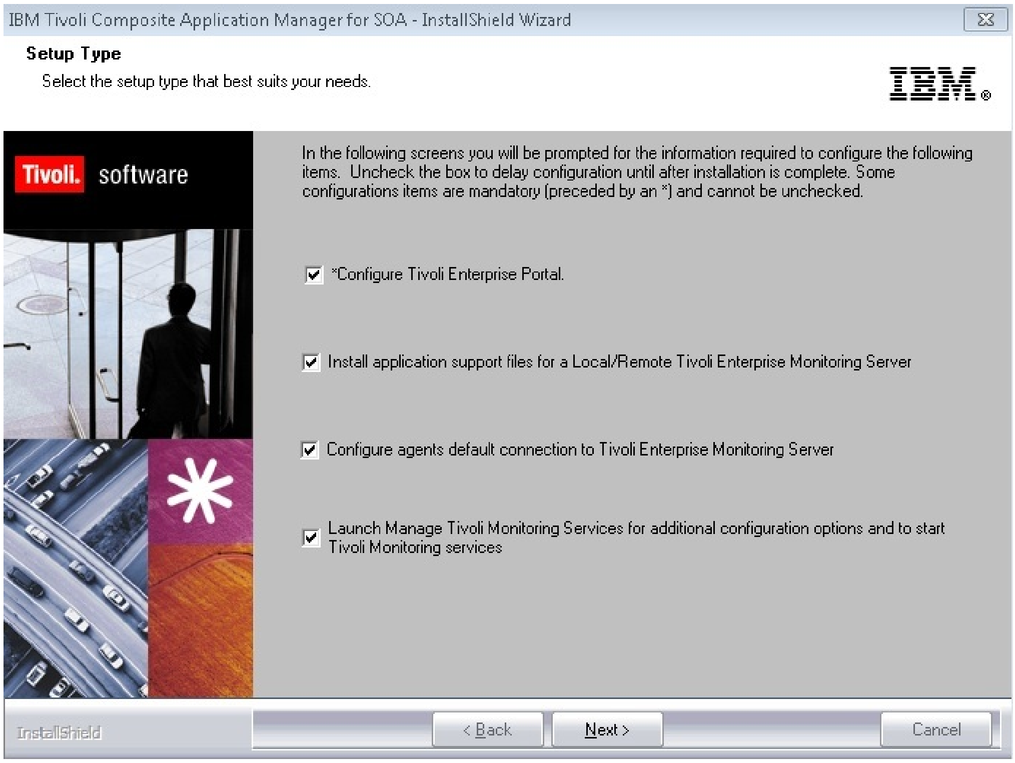
Figure 7. The Start Copying Files page

Important: If you are upgrading or updating from a previous version of ITCAM for SOA, you see a message that states that a previous installation has been detected and will be updated.

Review the installation summary details. The summary identifies what you are installing and where you choose to install it. Click **Next** to start the installation.

Step 9: Select the items to configure

When the features you selected are installed, the Setup Type window, similar to the following window, provides you with additional configuration options.


IBM Tivoli Composite Application Manager for SOA - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

In the following screens you will be prompted for the information required to configure the following items. Uncheck the box to delay configuration until after installation is complete. Some configurations items are mandatory (preceded by an *) and cannot be unchecked.

☑ *Configure Tivoli Enterprise Portal.

☑ Install application support files for a Local/Remote Tivoli Enterprise Monitoring Server

☑ Configure agents default connection to Tivoli Enterprise Monitoring Server

☑ Launch Manage Tivoli Monitoring Services for additional configuration options and to start Tivoli Monitoring services

Figure 8. The Setup Type page

The options presented here depend on whether IBM Tivoli Monitoring components are installed on the same computer system, whether application support is being installed, and whether the agents are being installed or upgraded.

Clear the check boxes of any components that are configured already (at the current release level) on this computer unless you want to modify the configuration.

Because the **Configure Tivoli Enterprise Portal** check box is selected, you are prompted to specify the host name of the Tivoli Enterprise Portal Server in a subsequent step.

If you see a **Install application support files for a Local/Remote Tivoli Enterprise Monitoring Server** check box and you choose this option, you are prompted to install application support files in a subsequent step.

If you see a **Configure agents default connection to Tivoli Enterprise Monitoring Server** check box and you choose this option, you are prompted to configure the default connection between the monitoring agent and the monitoring server as part of the installation of the monitoring agent in a subsequent step. For information about configuring the connection to the monitoring server, see "Configuring the monitoring agent" on page 58.

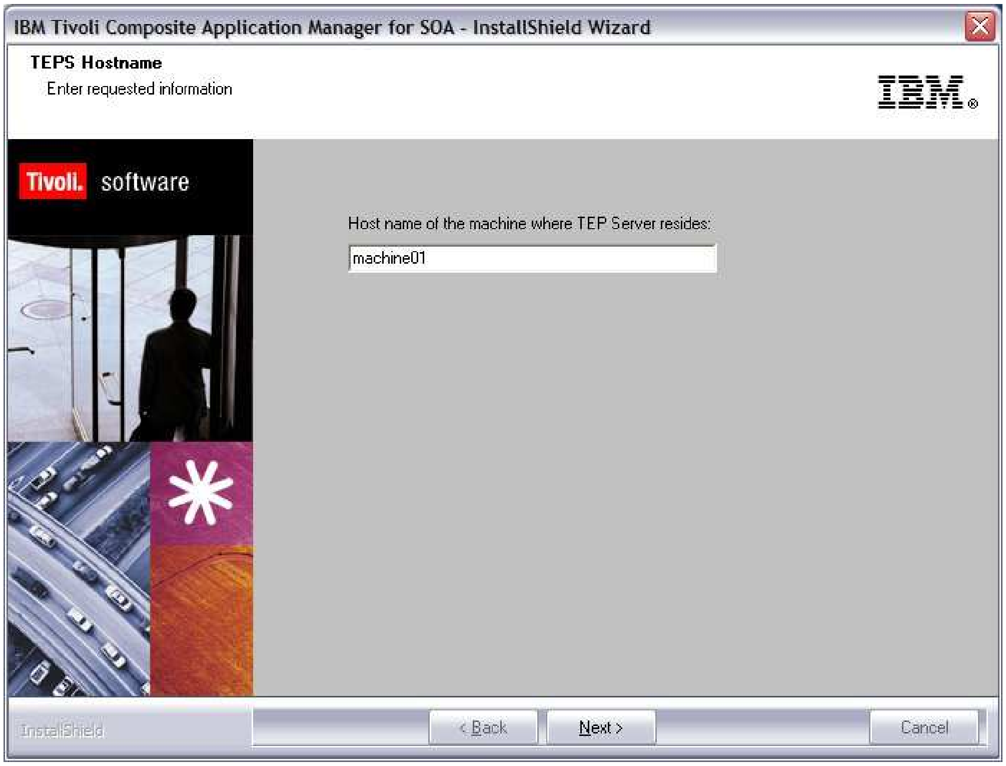
If you select the **Launch Manage Tivoli Services** check box, the Tivoli Monitoring utility starts after the installation of the monitoring agent completes. From this utility, you can configure the monitoring agent and other monitoring services to start automatically.

Click **Next**.

Step 10: Specify the host name of the portal server

If the option to configure the portal server was not selected in step "Step 9: Select the items to configure" on page 49, this step is skipped.

From the TEPS Hostname window, specify the host name of the Tivoli Enterprise Portal Server:


IBM Tivoli Composite Application Manager for SOA - InstallShield Wizard
TEPS Hostname
Enter requested information
IBM
Tivoli. software
InstallShield
< Back
Next >
Cancel

Host name of the machine where TEP Server resides: machine01

Figure 9. The TEPS Hostname page

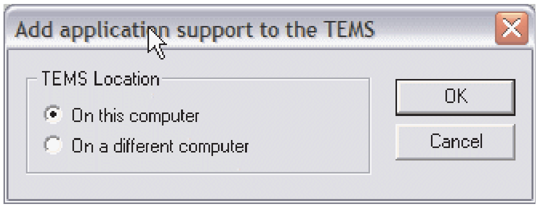
Click **Next**.

Step 11: Activate application support if IBM Tivoli Monitoring is installed

If you are not adding application support files to the Tivoli Monitoring components, skip this step.

If Tivoli Monitoring is installed on the same computer system and you are installing application support for the Tivoli Monitoring components, activate application support through a process that is known as seeding the monitoring server.

You are prompted to specify the location of the monitoring server to which to add application support:



Add application support to the TEMS

TEMS Location

● On this computer

○ On a different computer

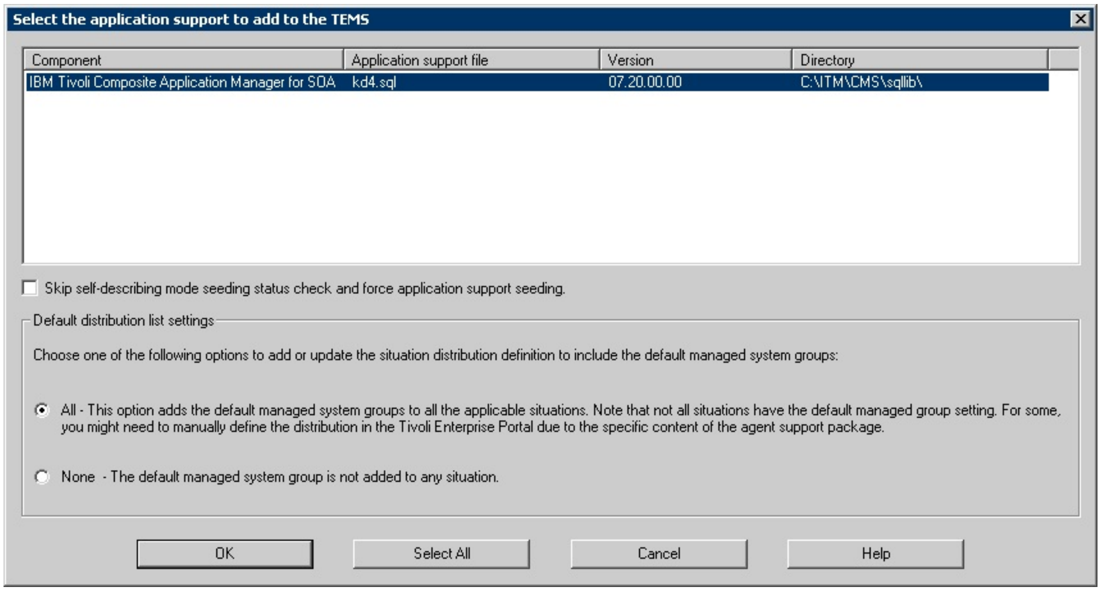
Figure 10. The Add application support to the TEMS Configuration page

Select **On this computer** and click **OK**.

Step 12: Add the default managed system list when you process application-support files

If you are not adding application support files to the Tivoli Monitoring components, skip this step.

You are prompted to add the default managed system list when you process the application support files.



Select the application support to add to the TEMS

Component	Application support file	Version	Directory
IBM Tivoli Composite Application Manager for SOA	kd4.sql	07.20.00.00	C:\ITM\CMS\sqllib\

□ Skip self-describing mode seeding status check and force application support seeding.

Default distribution list settings

Choose one of the following options to add or update the situation distribution definition to include the default managed system groups:

● All - This option adds the default managed system groups to all the applicable situations. Note that not all situations have the default managed group setting. For some, you might need to manually define the distribution in the Tivoli Enterprise Portal due to the specific content of the agent support package.

○ None - The default managed system group is not added to any situation.

Figure 11. The Add application support to the TEMS Configuration page

Select the All option to add the default managed systems groups to all applicable situations. Choose the None option if you do not want to add the default managed system group to any situation.

Click **OK**.

Step 13: View results of application support seeding process

If you are not adding application support files to IBM Tivoli Monitoring components, skip this step.

Click **Next** on the message that provides the result for the process of adding application support.

Step 14: Finalize the installation or upgrade

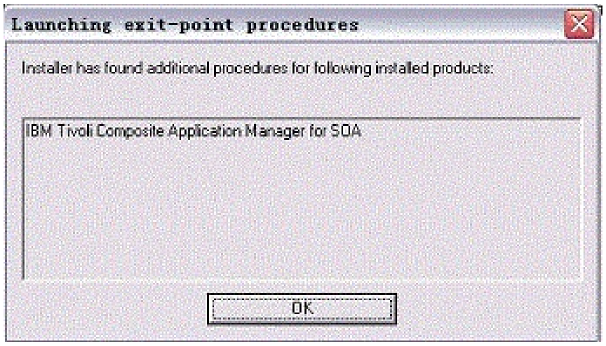
After you complete all configuration tasks, the InstallShield Wizard Complete page is displayed. If you do not want to read the product readme file for last-minute product information, clear the check box.

Click **Finish** to close the installer.

Click **Finish** on the Maintenance Complete window if you are updating an existing installation.

Step 15: Additional procedures in a pristine installation, upgrade, or update

A window is displayed to indicate that additional configuration procedures must be performed to complete the installation and configuration of the ITCAM for SOA agent.



Launching exit-point procedures

Installer has found additional procedures for following installed products:

IBM Tivoli Composite Application Manager for SOA

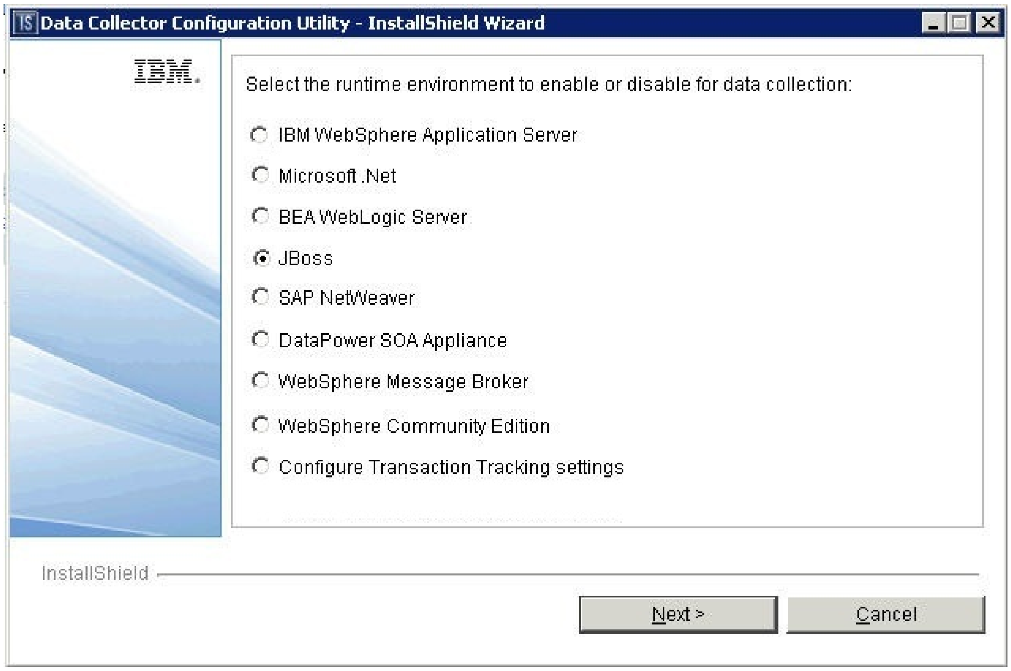
Figure 12. Message indicating that additional procedures were identified

Click **OK** to close this dialog and open the Data Collector Configuration utility for configuring data collectors in graphical user interface mode.

Step 16: Choose a runtime environment to configure for data collection

The Data Collector Configuration utility provides a list of runtime environments that can be configured for data collection.

When the Data Collector Configuration utility opens, you are prompted to select the appropriate language for the tool. You are also presented with a welcome page and a list of runtime environments for which data collection can be configured:



Select the runtime environment to enable or disable for data collection:

○ IBM WebSphere Application Server

○ Microsoft .Net

○ BEA WebLogic Server

● JBoss

○ SAP NetWeaver

○ DataPower SOA Appliance

○ WebSphere Message Broker

○ WebSphere Community Edition

○ Configure Transaction Tracking settings

Figure 13. Selecting a runtime environment to configure data collection

Tip: You cannot configure Data Collector for WebSphere Message Broker with this utility. The option **WebSphere Message Broker** is provided for disabling a previous version of the WebSphere Message Broker data collector.

If you are upgrading to ITCAM for SOA 7.2, or you want to postpone the configuration of data collectors, you can click **Cancel**. Skip to step "Step 20: Completing the installation and configuration of the data collector" on page 57 to complete the installation and configuration of the ITCAM for SOA monitoring agent.

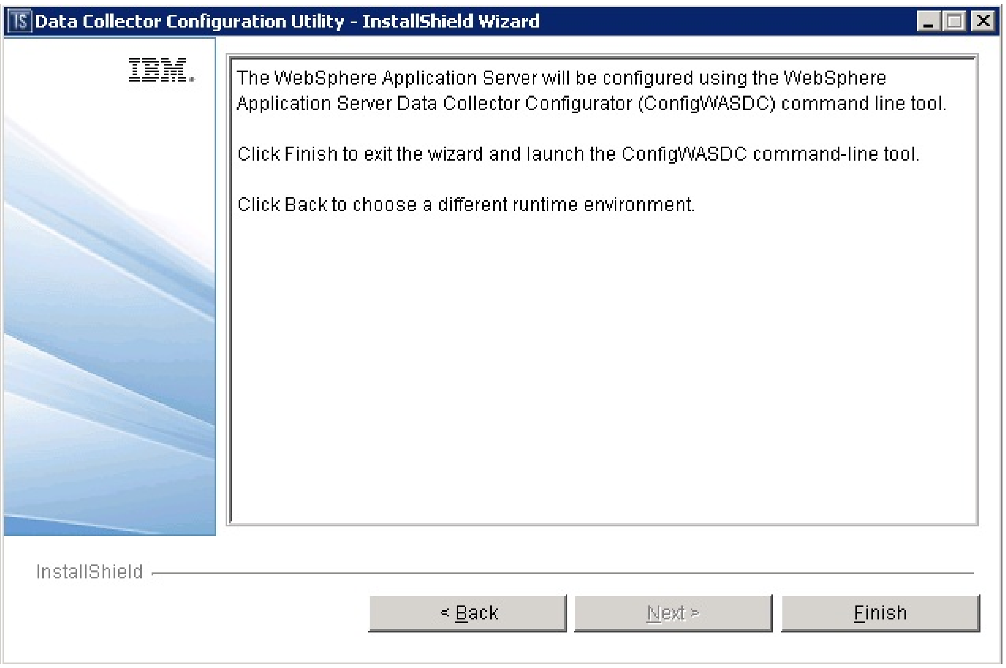
If you are installing or updating to ITCAM for SOA version 7.2 Fix Pack 1 and you are configuring data collection for a WebSphere Application Server environment, select **IBM WebSphere Application Server** to install and configure the ITCAM Data Collector for Websphere and click **Next**.

If the installer detects that the same version, release, and maintenance level of the ITCAM Data Collector for WebSphere is already installed on the computer system, the installation of the data collector is skipped.

All other data collectors are installed, upgraded, or updated as part of the installation of the ITCAM for SOA agent and can be configured with the Data Collector Configuration utility (see "Running the Data Collector Configuration utility graphical user interface" on page 379. If you are not configuring data collection for a WebSphere Application Server environment, optionally configure the data collector and skip to step "Step 20: Completing the installation and configuration of the data collector" on page 57 to complete the installation and configuration of the ITCAM for SOA monitoring agent.

Step 17: Confirm the installation of the ITCAM Data Collector for WebSphere

If you have chosen the option to perform a pristine installation, upgrade, or update of the WebSphere Application Server data collector in the Data Collector Configuration utility, you see a message that the WebSphere Application Server is configured with the ITCAM Data Collector for WebSphere Configuration utility in console mode.



The WebSphere Application Server will be configured using the WebSphere Application Server Data Collector Configurator (ConfigWASDC) command line tool.

Click Finish to exit the wizard and launch the ConfigWASDC command-line tool.

Click Back to choose a different runtime environment.

Figure 14. Message indicating that new ITCAM Data Collector for WebSphere Configuration utility is used to configure the Data Collector

Click **OK** to close the window. The command prompt window opens.

Step 18: Install ITCAM Data Collector for WebSphere

The ITCAM Data Collector for WebSphere in ITCAM for SOA version 7.2 and later is a component that is shared with the following products:

- ITCAM Agent for WebSphere Applications version 7.2
- ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5
- IBM Application Performance Diagnostics Lite
- ITCAM for Transactions

If ITCAM Agent for WebSphere Applications version 7.2 is already installed under the *ITM_home* directory or if you are performing a reinstallation, the same version, release, and maintenance level of the ITCAM Data Collector for WebSphere might be installed under *ITM_home*. If the installer detects that the ITCAM Data Collector for WebSphere is already installed under *ITM_home*, the installation of the data collector is skipped and the data collector configuration utility is displayed. Skip to step “Step 19: Configure the ITCAM Data Collector for WebSphere” on page 56.

Remember: The same version, release, and maintenance level of ITCAM Data Collector for WebSphere might be installed and configured for the same WebSphere profile, but the data collector installation might not be under the *ITM_home* directory:

- If the data collector is installed by ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 or Application Performance Diagnostics Lite, the data collector installation is outside of the *ITM_home* directory. The installer does not detect that the data collector already exists. When prompted, you must specify the location of the data collector installation.
- If the data collector is installed by ITCAM Agent for WebSphere Applications version 7.2 outside of *ITM_home*, the installer does not detect that the data collector exists. When prompted, you must specify the location of the data collector installation.

When the same version, release, and maintenance level of the data collector is not already installed under the *ITM_home* directory, the installer opens a command prompt window.

The installer prompts you to specify whether you want to:

- Install the data collector in the `DC_home` directory (default install)
- Reuse an existing data collector home directory (custom install)
- Create a new data collector home directory (custom install)

```
Choose the type of install to perform.
      1. default install
      2. custom install
[default is: 1]:
```

Enter 1 to install the data collector in the *DC_home* directory.

Otherwise, enter 2 and specify the location of the data collector home directory. If the installer finds that the data collector home directory does not exist, it asks you whether you want to create the directory.

```
Directory C:\IBM\ITM\dchome\7.2.0.0.4 does not exist.  Is it ok to create?
[1 - YES, 2 - NO]
```

Enter 1 to create the directory. If you enter 2, you can enter a different data collector home directory or exit the command prompt.

Restriction: You must not install the data collector in the same directory where version 7.1.1 of the ITCAM for SOA WebSphere Application Server data collector is installed.

If the data collector installation does not already exist, the installer starts the installation of the data collector.

Step 19: Configure the ITCAM Data Collector for WebSphere

If you are configuring the data collector only for an ITCAM for SOA environment, you must integrate the data collector at least with ITCAM for SOA, and optionally, integrate the data collector with ITCAM for Transactions. For description of the steps to follow when configuring the data collector with the ITCAM Data Collector for WebSphere Configuration utility, see "Configuring ITCAM Data Collector for WebSphere" on page 274.

If you are installing ITCAM for SOA and you want to postpone the configuration of the ITCAM Data Collector for WebSphere until later, you can exit the utility. At a later time, use the ITCAM Data Collector for WebSphere Configuration utility to configure the data collector.

If the data collector component of an older version of any of the following products is configured within the same profile, exit the utility, and migrate the data collector:

- Older versions of the ITCAM Agent for WebSphere Applications, including:
  – ITCAM Agent for WebSphere Applications version 7.1
  – ITCAM for WebSphere version 6.1.0.4 or later
  – WebSphere Data Collector version 6.1.0.4 or later component of ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM for WebSphere Application Server version 7.2

For the migration procedure, see “Migrating data collectors to ITCAM Data Collector for WebSphere” on page 291.

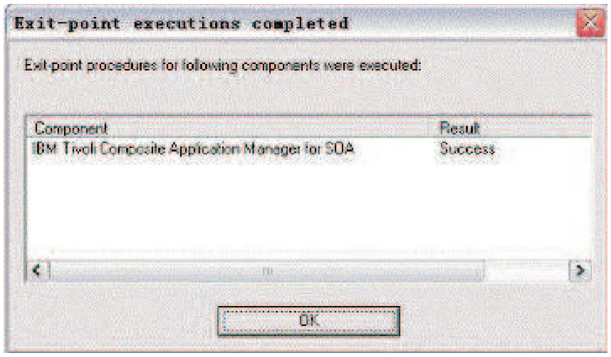
If an older version of ITCAM for SOA is configured for the same profile, exit the utility, and migrate the data collector (see “Migrating data collectors to ITCAM Data Collector for WebSphere” on page 291).

If an earlier maintenance level of the ITCAM Data Collector for WebSphere is configured for the same profile, exit the utility, and migrate the data collector (see “Migrating data collectors to ITCAM Data Collector for WebSphere” on page 291.

For a description of considerations when installing and configuring IBM Business Process Monitoring considerations, an overview of installation and upgrade scenarios, and procedures for running the configuration utilities in interactive and silent modes, see Chapter 7, “Configuring data collection: WebSphere Application Server,” on page 257.

Step 20: Completing the installation and configuration of the data collector

When you exit the Data Collector Configuration utility, a message is displayed to indicate that the additional data collector configuration procedure completed successfully:



Exit-point executions completed

Exit-point procedures for following components were executed:

Component	Result
IBM Tivoli Composite Application Manager for SOA	Success

Figure 15. Message confirmation that configuration of data collector is complete

The message is displayed only if the Data Collector Configuration utility started automatically after the installation of the monitoring agent.

Important: If you cancel the configuration of the ITCAM Data Collector for WebSphere after it is installed, the message displays the value `Error` in the result column. This message indicates that the data collector is installed but is not configured.

Step 21: Verifying the installation of the monitoring agent

To verify that the installation was successful, open the Manage Tivoli Enterprise Monitoring Services Utility (if it does not open automatically) to see whether the monitoring agent that you upgraded is configured and started. To open the utility, enter the Windows **Start Menu** and click **Programs** > **IBM Tivoli** > **Monitoring** > **Manage Tivoli Monitoring Services** to start the utility. If **Yes** is displayed in the **Configured** column, the monitoring agent was configured and started during the upgrade process.

Step 22: Preparing the Tivoli Enterprise Portal browser client

After you install, upgrade, or update ITCAM for SOA, the user interface might not display properly when you view it from a Tivoli Enterprise Portal browser client. Before starting the Tivoli Enterprise Portal, you must clear the cache of your web browser and your IBM Java plug-in. To clear the cache, complete the following steps:

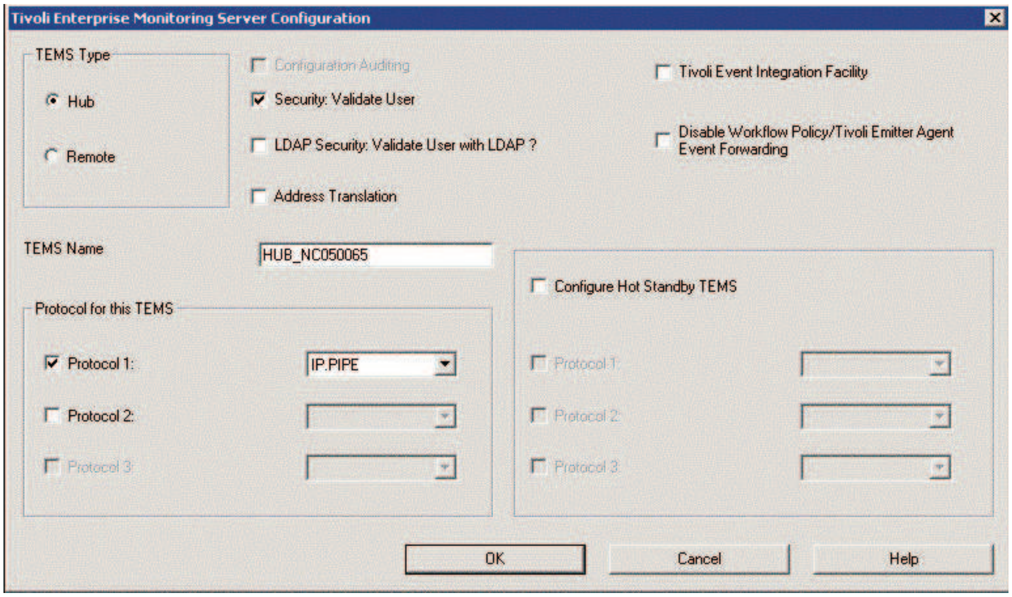
1. From your browser client, clear all temporary files, cookies, and history files.
2. To clear the Java plug-in, complete the following steps:
   a. Double-click **IBM Control Panel for Java** to start the Java control program.
   b. On the **General** tab, click **Settings** in the **Temporary Internet Files** section.
   c. On the **Temporary Files Settings** dialog, click **Delete Files**.
   d. Click **OK** to close the Java control panel.

Configuring the monitoring agent

As part of the installation or upgrade of the monitoring agent, if you selected the **Configure agents default connect to Tivoli Enterprise Monitoring Server**, the agent configuration window opens automatically as part of the installation or upgrade. Otherwise, to open the Agent Configuration window from the Manage Tivoli Monitoring Services utility.

To open the Agent Configuration window, complete these steps:

1. Enter the Windows **Start Menu** and click **Programs** > **IBM Tivoli** > **Monitoring** > **Manage Tivoli Monitoring Services**. The Manage Tivoli Monitoring Services utility is displayed.
2. Right-click the agent and select **Reconfigure**. A window for configuring the Tivoli Enterprise Monitoring Server connection window is displayed.


Tivoli Enterprise Monitoring Server Configuration

TEMS Type

● Hub

○ Remote

□ Configuration Auditing

☑ Security: Validate User

□ LDAP Security: Validate User with LDAP ?

□ Address Translation

□ Tivoli Event Integration Facility

□ Disable Workflow Policy/Tivoli Emitter Agent Event Forwarding

TEMS Name: HUB_NC050065

Protocol for this TEMS

☑ Protocol 1: IP.PIPE

□ Protocol 2:

□ Protocol 3:

□ Configure Hot Standby TEMS

□ Protocol 1:

□ Protocol 2:

□ Protocol 3:

Figure 16. Tivoli Enterprise Monitoring Server Configuration

To configure the connection between the monitoring agent and the monitoring server, complete these steps.

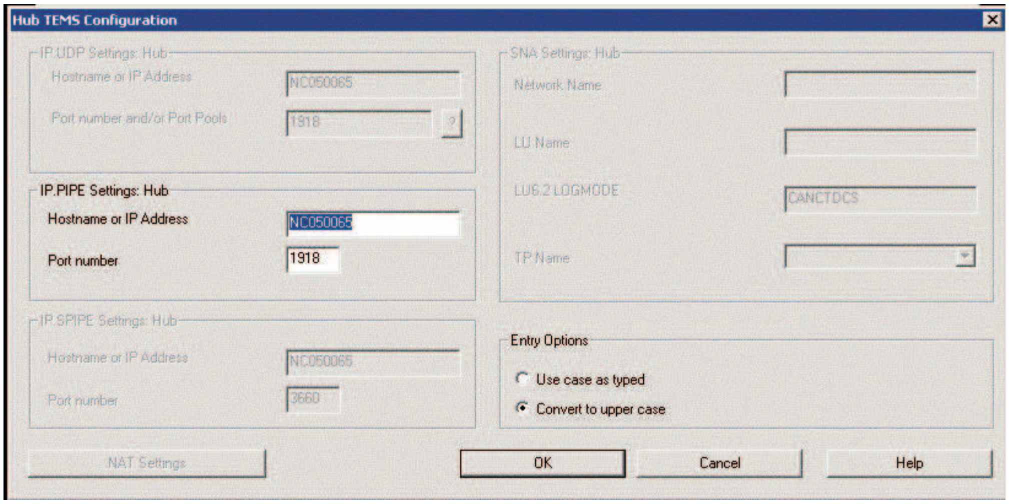
1. In the Tivoli Enterprise Monitoring Server Configuration window, if the monitoring server connection is already configured, you do not have to change the configuration. Click **OK**.

   To configure the monitoring server connection, identify the protocol that the monitoring agent uses to communicate with the hub monitoring server. You have five choices:

   - `IP.UDP`
   - `IP.PIPE`
   - `IP.SPIPE`
   - `SNA`
   - `No TEMS`

   The value that you specify here must match the value that is specified when you install the monitoring server. You can also set a secondary protocol if required.

   Click **OK**.
2. The Hub TEMS Configuration window is displayed.



Hub TEMS Configuration

IP.UDP Settings: Hub
Hostname or IP Address: NC050065
Port number and/or Port Pools: 1918

IP.PIPE Settings: Hub
Hostname or IP Address: NC050065
Port number: 1918

IP.SPIPE Settings: Hub
Hostname or IP Address: NC050065
Port number: 3660

SNA Settings: Hub
Network Name:
LU Name:
LU6.2 LOGMODE: CANCTDCS
TP Name:

Entry Options
○ Use case as typed
● Convert to upper case

Figure 17. Hub Tivoli Enterprise Monitoring Server Configuration

For the protocol or protocols that you selected in the previous window, specify these fields as explained in Table 7.

Table 7. Protocol settings for communicating between the monitoring agent and the monitoring server

Protocol	Field	Description
IP.UDP	Hostname or IP address	The host name or IP address for the monitoring server to which the monitoring agent is connected.
	Port # and/or Port Pools	The listening port for the monitoring server to which the monitoring agent is connected. The default value is 1918.
IP.PIPE	Hostname or IP Address	The host name or IP address for the monitoring server to which the monitoring agent is connected.
	Port # and/or Port Pools	The listening port for the monitoring server. The default value is 1918.
IP.SPIPE	Hostname or IP Address	The host name or IP address for the monitoring server to which the monitoring agent is connected.
	Port Number	The listening port for the monitoring server to which the monitoring agent is connected. The default value is `3660`.
SNA	Network Name	The SNA network identifier for your location.
	LU Name	The LU name for the Tivoli Enterprise Monitoring Server. This LU name corresponds to the local LU Alias in your SNA communications software.
	LU 6.2 LOGMODE	The name of the LU6.2 LOGMODE. The default value is `CANCTDCS`.
	TP Name	The transaction program name for the monitoring server.
	Local LU Alias	The LU alias.

Click **OK**.

For more information about configuring the connection to the monitoring server, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Silent installation on Windows systems

In addition to installing the ITCAM for SOA agent interactively, the installer supports a silent mode. In this mode, no user interaction is required for an installation or uninstallation. Instead, the parameters are taken from a *response* file. You can install and uninstall the ITCAM for SOA agent and install application support files in silent mode.

Response files have a text format. You can create a response file that is based on one of the samples provided on the installation DVD or image.

You can also create a response file during installation, modify it if necessary, and then use it for a silent installation. In this way, you can reproduce similar configuration many times, for example, on different hosts.

Preparing response files on Windows systems

You can use the installer to install or uninstall the ITCAM for SOA agent in silent mode. You can also install application support files for the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal client on Windows in silent mode. Modify the sample response files that are on the installation DVD or image, and then run the installer from the command line.

For information about installing the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal in silent mode, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

To perform a silent installation or uninstallation of the monitoring agent and application support files, you must first prepare the response file. Then, run the installer, supplying the name of the response file.

Preparing the response file for ITCAM for SOA agent installation

To prepare a response file for installing the ITCAM for SOA agent, complete the following procedure:

1. On the product installation DVD or image, in the `WINDOWS\Deploy` directory, locate the `D4_Silent_Install.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify any of the following properties, if necessary. Do not modify any other properties.

Table 8. ITCAM for SOA installation response file properties

Parameter	Definition
Install Directory	Required. Assign the full path name of the directory for the monitoring agent if it is different from the default. The default is `C:\IBM\ITM`. If you are installing on a computer where the monitoring agent is already installed, the current directory is used regardless of what you specify here.
Install Folder	Required. Assign the name of the folder that is displayed in the Windows **Start** > **Programs** menu. Use this option if you want to use a folder name different from the default.
EncryptionKey	Required. The data encryption key that is used to encrypt the data that is sent between systems. This key must be the same for all components in your Tivoli Monitoring environment.

4. Save the edited copy in a work directory, for example, as `C:\TEMP\silent_install.txt`.

Preparing the response file for ITCAM for SOA agent uninstallation

To prepare a response file for uninstallation of the ITCAM for SOA agent, perform the following procedure:

1. On the product installation DVD or image, in the `WINDOWS\Deploy` directory, locate the `D4_Silent_Uninstall.txt` file.
2. Copy the file to a work directory, for example, as `C:\TEMP\silent_install.txt`. Do not modify the copy.

Remember: If the ITCAM Data Collector for WebSphere home directory was specified to be outside of the Tivoli Monitoring home directory, the ITCAM Data Collector for WebSphere home directory is not removed during the uninstallation.

Preparing the response file for application support files installation

To prepare a response file for installing the support files on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal client, complete the following procedure:

1. On the product installation DVD or image, in the `WINDOWS` directory, locate the `silent.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Find the following lines, and uncomment the lines that apply to the host that you are installing on:
   ```
   KD4WICMS=ITCAM for SOA Support ( TEMS )
   KD4WIXEW=ITCAM for SOA Support ( TEP Workstation )
   KD4WICNS=ITCAM for SOA Support ( TEP Server )
   KGLWICMA=Tivoli Enterprise Monitoring Agent Framework
   ```
4. Save the edited copy in a work directory, for example, as `C:\TEMP\silent_install.txt`.

Running the silent installation from a command prompt with parameters

Complete the following steps to run the installation from the command line:

1. From a command prompt, change to the directory that contains this installation (where the `setup.exe` and `setup.ins` files are located).
2. Run the setup as follows. You must specify the parameters in the same order as listed.
   ```
   start /wait setup /z"/sfC:\temp\silent_file" /s
   /f2"C:\temp\silent_setup.log"
   ```
   Where:

   silent_file
   Name of the silent file, for example, silent_install.txt

   /z"/sf" Specifies the name and location of the installation driver that you customized for your site. This parameter is a required parameter. This file must exist.

   /s Specifies that this installation is a silent installation. If you specify this option, nothing is displayed during the installation.

/f2 Specifies the name of the Install Shield log file. If you do not specify this parameter, the default is to create the `setup.log` file in the same location as the `setup.iss` file. In either case, the Setup program must be able to create and write to the log file.

Running the silent installation with SMS

Complete the following steps to run the installation with SMS:

1. Copy all of the installation files to a LAN-based disk that SMS mounts on the specified computers. Copy all the files in the directory that contains the `setup.exe` and `setup.ins` files.
2. Replace the original `silent_install.txt` file on the LAN disk with your modified version.
3. Edit the PDF file that is located with the `setup.exe` file and change the Setup call as follows:

   ```
   Setup /z"/sfC:\temp\silent_install.txt" /s /f2"C:\temp\silent_setup.log"
   ```

For information about a silent installation of Tivoli Monitoring, see "Appendix B. Performing a silent installation of IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Configuring for remote deployment of the monitoring agent

The ITCAM for SOA supports the Tivoli Monitoring feature of remotely deploying the monitoring agent across your environment from a central location, the monitoring server.

Before you install the ITCAM for SOA monitoring agent on a remote system using Tivoli Enterprise Portal, the application support files must be installed on the Tivoli Enterprise Portal Server (including browser client support files), hub and remote Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal desktop clients.

Installation of application support files is only required when the monitoring agent is deployed from the Tivoli Enterprise Portal, However, the application support files must be installed to view monitoring data in the Tivoli Enterprise Portal, regardless of whether the agent was installed remotely with the Tivoli Enterprise Portal or from the command-line interface.

The application support files are automatically propagated to the monitoring server if the following conditions are met:

1. Self-description is enabled on the hub and remote monitoring servers
2. All Tivoli Management Services server components are at version 6.2.3 or higher.
3. The agent framework is at version 6.2.3 or higher.

Self-description is enabled by default on the ITCAM for SOA. For more information about the conditions that must be met for self-description, see "Enabling application support through self-description" on page 36.

Important: Remote deployment of ITCAM for SOA to a remote Windows 7 platform is not supported.

For more information about remote deployment in an IBM Tivoli Monitoring environment, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Adding the installation bundles to the deployment depot

Before you can deploy a monitoring agent to a remote computer, you must add the operating system-specific monitoring agent bundle to the deployment depot. For example, if you are deploying monitoring agents to a Windows operating system, the Windows system bundle must be added to the deployment depot.

If you installed application support files for the monitoring server, you might have added the monitoring agents to the deployment depot during the installation. If not, you can add a monitoring agents bundle to the deployment depot at any time with the following method:

1. Copy or mount the ITCAM for SOA monitoring agent installation images on the monitoring server host.
2. Change to the `*ITM_HOME*\bin` directory.
3. Use the following command to log in to the monitoring server:

   ```
   tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user and the password for the SYSADMIN user. For example:

   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```

4. (Optional) List the available bundles in the *path_to_Windows_image*`\Windows\deploy` directory with the following command:

   ```
   tacmd listBundles -i path_to_Windows_image\Windows\deploy
   ```

   You might receive a reply similar to the following message:

   ```
   Product Code : D4
   Version      : 072000000
   Description  : Monitoring Agent for Composite Application Manage for SOA
   Host Type    : WINNT
   Host Version : WINNT
   Prerequisites:
   ```

5. To add the installation bundle for Windows target hosts, enter this command:

   ```
   tacmd addBundles -i path_to_Windows_image\WINDOWS\Deploy -t d4
   ```

   The code `d4` is the product code for the ITCAM for SOA monitoring agent. You might receive a reply similar to the following, where *Depot_dir* is the location where the deployment depot is located, for example, `C:\IBM\ITM\CMS`:

   ```
    KUICAB023I : Are you sure you want to add the following bundles to the
   <Depot_dir>\depot\ depot?

   Product Code : D4
   Version      : 072000000
   Description  : Monitoring Agent for Composite Application Manage for SOA
   Host Type    : WINNT
   Host Version : WINNT
   Prerequisites:
    KUICAB024I : Enter Y for yes or N for no:
   ```

   Enter `Y` to add the agent bundle to the deployment depot. Wait for the process to complete. A confirmation message is displayed when the bundle is added. You can use the **`tacmd viewDepot`** command to display the bundles that were added to the deployment depot.

For more information about this procedure, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing the ITCAM for SOA monitoring agent remotely with Tivoli Enterprise Portal

You can use the Tivoli Enterprise Portal to install the monitoring agent remotely.

Before you install the ITCAM for SOA monitoring agent on a remote system, the application support files must be installed on the Tivoli Enterprise Portal Server (including the browser client support files), hub and remote Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal desktop clients.

Before you can install the ITCAM for SOA monitoring agent on a remote system, you must first deploy an OS monitoring agent to the remote system. See the *Tivoli Monitoring: Installation and Setup Guide* for details.

To install the monitoring agent remotely with Tivoli Monitoring, complete the following procedure:

1. From the physical Navigator view in the Tivoli Enterprise Portal, navigate to the computer where you want to install the monitoring agent.
2. Right-click the remote computer and select **Add Managed System**.
3. Select **Monitoring Agent for Composite Application Manager for SOA** and click **OK**.
4. The New Managed System Configuration window is displayed. Accept the default to use the local system account or specify a valid account and password.
5. Click **Finish**. The monitoring agent installation process is started; you can track its progress in the Deployment Status workspace.

This procedure installs the monitoring agent and the ITCAM for SOA-specific data collectors.

Restriction: The procedure does not install the Data Collector for WebSphere Message Broker. To install the Data Collector for WebSphere Message Broker on a remote system, copy the ITCAM for SOA installation media to the remote system, run the installation wizard, and select the Data Collector for WebSphere Message Broker from the list of features that are available for installation.

To install and configure the ITCAM Data Collector for WebSphere, see "Installing and configuring ITCAM Data Collector for WebSphere from a command prompt" on page 66.

For more information about remotely installing an agent from the Tivoli Enterprise Portal, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing the ITCAM for SOA monitoring agent remotely from a command prompt

You can install the monitoring agent to a remote system from the command prompt of the monitoring server.

Before you can install the ITCAM for SOA monitoring agent on a remote system, you must first deploy an OS monitoring agent to the remote system. See the *Tivoli Monitoring: Installation and Setup Guide* for details.

You do not have to install application support files on the Tivoli Enterprise Portal Server, hub and remote Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal desktop clients before you install the agent remotely from the command prompt. However, the application support files must be installed to view monitoring data in the Tivoli Enterprise Portal after remote deployment.

For details on using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

To install the monitoring agent with the command prompt, perform the following procedure on the monitoring server:

1. Change to the *ITM_HOME*`\bin` directory.

   For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
2. Use the following command to log in to the monitoring server:
   ```
   tacmd login -s TEMS_hostname -u userid -p password
   ```
   Use the SYSADMIN user of Tivoli Monitoring and password. For example:
   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
3. To install the ITCAM for SOA monitoring agent on a remote host, enter the **tacmd addSystem** command. Specify `d4` as the product code for the ITCAM for SOA monitoring agent. Specify the node name. The name of the node includes the computer where the OS agent is installed and the product code for the OS agent.
   ```
   tacmd addSystem -t d4 -n Primary:SOAWIN48:NT
   ```
4. If you want to monitor the remote deployment status, enter the following command:
   ```
   tacmd getDeployStatus
   ```
   The monitoring agent and the ITCAM for SOA data collectors are installed.

For more information about remotely installing an agent from a command prompt, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

This procedure installs the monitoring agent and the ITCAM for SOA-specific data collectors.

Restriction: The procedure does not install the Data Collector for WebSphere Message Broker. To install the Data Collector for WebSphere Message Broker on a remote system, copy the ITCAM for SOA installation media to the remote system, run the installation wizard, and select the Data Collector for WebSphere Message Broker from the list of features that are available for installation.

To install and configure the ITCAM Data Collector for WebSphere, see "Installing and configuring ITCAM Data Collector for WebSphere from a command prompt."

When the monitoring agent is successfully installed, it connects automatically to the monitoring server, and the portal desktop displays it.

Installing and configuring ITCAM Data Collector for WebSphere from a command prompt

You can install and configure ITCAM Data Collector for WebSphere on a remote system using `tacmd` commands from the command prompt of the monitoring server.

You must install the monitoring agent on the remote system before you install ITCAM Data Collector for WebSphere.

When you install monitoring agent on the remote system, ITCAM Data Collector for WebSphere installation files are placed in the *ITCAM4SOA_Home*\wasdc directory. For example C:\IBM\ITM\TMAITM6\KD4\wasdc. The directory contains the following files:

- Data collector installation files, itcam_gdc.zip.
- A script to extract and install the installation files, gdc_extract.bat.

For more information about operating system-dependent variables, see "Operating system-dependent variables and paths" on page xv.

Tip: In the following procedure, if the monitoring server is on a Windows system, use the tacmd command. If the monitoring server is on a Linux or UNIX system, use the ./tacmd command.

You can use tacmd executecommand to install the data collector and configure it in silent mode. To use the tacmd executecommand command, the hub and remote monitoring servers must be at version 6.2.2 fix pack 2 or later. For details about using tacmd commands, see *IBM Tivoli Monitoring Command Reference*.

To install the ITCAM Data Collector for WebSphere from the command line, complete the following procedure on the monitoring server:

1. Change to *ITM_HOME*\bin directory.
2. Use the following command to log in to the monitoring server:

   ```
   tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```

3. Set the KT1_TEMS_SECURE configuration parameter in the hub monitoring server's configuration file to specify that the hub monitoring server supports the tacmd commands:
   - Navigate to the file *ITM_HOME*\CMS\KBBENV.
   - Add the property KT1_TEMS_SECURE='YES', if it does not exist.
   - Recycle the hub monitoring server
4. Set the location of the Java home directory, the Tivoli Monitoring home directory, and the data collector home directory. Extract the data collector installation files to the data collector home directory.

```
 tacmd executecommand -m System -c "set JAVA_HOME=path_to_java_home&set CANDLE_HOME=path_to_ITM_home&
gdc_extract.bat -d path_to_dc_home full_path_to_archive_file" -w CAM4SOA_Home\wasdc
```

Where:

-m|--system
Specifies on which managed system to run the command.

-c|--commandstring
Specifies the command to run. Use double quotation marks for commands with parameters. You must escape back slashes when defining a Windows directory path. For more information, see the "Escaping backslashes, spaces, and double quotation marks" section in the *Tivoli Monitoring Command Reference* guide.

-w|--workingdir
Specifies the working directory that is switched to before the command is run. When running this command between a UNIX or Linux system and targeting a Windows monitoring agent, you must replace the backslashes with forward slashes in the path definitions for the source

parameter. It is best to use forward slashes for tolerance with Windows systems. If the working directory contains spaces, you must include double quotation marks around the directory location.

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "set JAVA_HOME=C:\IBM\WebSphere\AppServer\java&set
CANDLE_HOME=C:\IBM\ITM&gdc_extract.bat -d C:\\IBM\\ITM\\dchome C:\\IBM\\ITM\\TMAITM6\\KD4\\wasdc\\
itcam_gdc.zip"
-w C:\\IBM\\ITM\\TMAITM6\\KD4\\wasdc
```

Important: In interactive mode, the user is expected to press any key to continue to indicate to the batch file that the script is complete. The command might return a non-zero when it is run in console mode on a remote system, although the `gitcam_gdc.zip` file is extracted successfully.

5. Specify the data collector configuration in a properties file on the monitoring server. A sample properties file, `sample_silent_config.txt`, is available from *DC_home*`\bin` on any local system where you installed the agent.
6. Copy the *silent_file* from the monitoring server to the remote system using the `tacmd putfile` command.

```
tacmd putfile -m System -s local_dir_path\silent_file -d remote_dir_path\silent_file -t text
```

Where:

-m|--system
Specifies on which managed system to run the command.

-s|--source
Specifies the local file name.

-d|--destination
Specifies the remote file name.

-t|--text
Specifies the mode of transfer.

For example:

```
tacmd putfile -m Primary:WINDOWS:NT -s /opt/IBM/ITM/dchome/silent_file.txt
-d c:\\temp\\silent_file.txt -t text
```

7. Configure the data collector using the response silent response file:

```
tacmd executecommand -m System -c "config.bat -silent full_path_to_silent_file\\silent_file.txt" -w path_to_DC_home\bin
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "config.bat -silent C:\\temp\\silent_file.txt"
-w C:\\IBM\\ITM\\dchome\\7.2.0.0.4\\bin
```

8. Restart the application server instances.
   a. Stop the application server.

```
tacmd executecommand -m System -c "stopServer.bat server_name" -w profile_home\bin
```

   For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "stopServer.bat server1"
-w C:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01\\bin
```

   b. Start the application server:

```
tacmd executecommand -m System -c "startServer.bat server_name -w profile_home\bin"
```

   For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "startServer.bat server1"
-w C:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01\\bin
```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Upgrading a remotely deployed ITCAM for SOA monitoring agent

To upgrade or update an existing remotely deployed ITCAM for SOA monitoring agent on a specified managed system to a newer version, add the new version of the monitoring agent to the deployment depot and then use the **`tacmd updateAgent`** command to upgrade the monitoring agent. This command is documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Remember: ITCAM for SOA supports only a single installation per computer system.

You might already have a previous version (version 7.1.1 or version 7.2) of the ITCAM for SOA monitoring agent deployed to a remote system in your environment. With the remote agent deployment function of Tivoli Monitoring, you can populate the deployment depot with newer versions of your monitoring agent and use the remote deployment function to upgrade or update to the newer version.

Before you can remotely deploy a newer version of the monitoring agent, you must first deploy an OS agent to the remote system. Deploy this OS agent to the same Tivoli Monitoring installation directory (*ITM_home*) as the installation directory of the existing version of the ITCAM for SOA monitoring agent. When you deploy the new version of the monitoring agent, you must also specify the same directory where the OS agent is installed. This ensures that the previous version of the monitoring agent is upgraded.

This procedure upgrades or updates the ITCAM for SOA monitoring agent and the ITCAM for SOA-specific data collectors.

To migrate the ITCAM Data Collector for WebSphere, see "Migrating to ITCAM Data Collector for WebSphere from a command prompt."

To migrate the WebSphere Message Broker data collector, you must copy the agent installation media to the remote system, and follow the upgrade procedure in "Upgrading to the Data Collector for WebSphere Message Broker" on page 360.

Migrating to ITCAM Data Collector for WebSphere from a command prompt

When you upgrade to ITCAM for SOA version 7.2 or later on the remote system, there may be other older versions of the data collector installed and configured for the same profile in which you plan to configure ITCAM for SOA.

These older versions of the data collector must be migrated to the ITCAM Data Collector for WebSphere after you install ITCAM Data Collector for WebSphere. The ITCAM for SOA 7.1.1 data collector for the WebSphere Application Server is upgraded automatically as part of the migration of these older versions of the data collector.

When an earlier maintenance level of the ITCAM Data Collector for WebSphere is installed and configured for the same profile, you can migrate it to the latest maintenance level using the ITCAM Data Collector for WebSphere Migration utility.

You can use `tacmd executecommand` to migrate older versions and earlier maintenance levels of the data collector in silent mode. For details about using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

In the following procedure, if the monitoring server is on a Windows system, use the `tacmd` command. If the monitoring server is on a Linux or UNIX system, use the `./tacmd` command.

To migrate an older version or an earlier maintenance level of the data collector to the latest ITCAM Data Collector for WebSphere, complete the following procedure from the command prompt of the monitoring server:

1. Change to *ITM_HOME*`\bin` directory.
2. Use the following command to log in to the monitoring server:

   ```
   tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
3. Set the `KT1_TEMS_SECURE` configuration parameter in the hub monitoring server's configuration file to specify that the hub monitoring server supports the `tacmd` commands:
   - Navigate to the file *ITM_HOME*`\CMS\KBBENV`.
   - Add the property `KT1_TEMS_SECURE='YES'`, if it does not exist.
   - Recycle the hub monitoring server
4. Set the location of the Java home directory, the Tivoli Monitoring home directory, and the data collector home directory. Extract the data collector installation files to the data collector home directory.

```
 tacmd executecommand -m System -c "set JAVA_HOME=path_to_java_home&set CANDLE_HOME=path_to_ITM_home&
gdc_extract.bat -d path_to_dc_home full_path_to_archive_file" -w CAM4SOA_Home\wasdc
```

Where:

-m|--system
: Specifies on which managed system to run the command.

-c|--commandstring
: Specifies the command to run. Use double quotation marks for commands with parameters. You must escape back slashes when defining a Windows directory path. For more information, see the “Escaping backslashes, spaces, and double quotation marks” section in the *Tivoli Monitoring Command Reference* guide.

-w|--workingdir
: Specifies the working directory that is switched to before the command is run. When running this command between a UNIX or Linux system and targeting a Windows monitoring agent, you must replace the backslashes with forward slashes in the path definitions for the source parameter. It is best to use forward slashes for tolerance with Windows systems. If the working directory contains spaces, you must include double quotation marks around the directory location.

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "set JAVA_HOME=C:\IBM\WebSphere\AppServer\java&set
CANDLE_HOME=C:\IBM\ITM&gdc_extract.bat -d C:\\IBM\\ITM\\dchome C:\\IBM\\ITM\\TMAITM6\\KD4\\wasdc\\
itcam_gdc.zip"
-w C:\\IBM\\ITM\\TMAITM6\\KD4\\wasdc
```

Important: In interactive mode, the user is expected to press any key to continue to indicate to the batch file that the script is complete. The command might return a non-zero when it is run in console mode on a remote system, although the `itcam_gdc.zip` file is extracted successfully.

5. Specify the migration details in a properties file on the monitoring server. Two sample properties file are available from *DC_home*`\bin` on any local system where you installed the agent.

   The file, `sample_silent_migrate.txt`, can be used when you migrate the data collector of the following products to the ITCAM Data Collector for WebSphere:
   - ITCAM for WebSphere 6.1.0.4 or later
   - WebSphere Data Collector 6.1.0.4 or later included in ITCAM for Web Resources 6.2.0.4 or later
   - ITCAM Agent for WebSphere Applications 7.1 included in ITCAM for Applications Diagnostics 7.1
   - ITCAM for WebSphere Application Server 7.2

   The file, `sample_silent_migrate_soa.txt`, can be used when you migrate the ITCAM for SOA 7.1.1 data collector to the ITCAM Data Collector for WebSphere.
6. Copy the *silent_file* from the managing server to the remote system using the `tacmd putfile` command.

```
tacmd putfile -m System -s local_dir_path\silent_file -d remote_dir_path\silent_file -t text
```

Where:

-m|--system
Specifies on which managed system to run the command.

-s|--source
Specifies the local file name.

-d|--destination
Specifies the remote file name.

-t|--text
Specifies the mode of transfer.

For example:

```
tacmd putfile -m Primary:WINDOWS:NT -s /opt/IBM/ITM/dchome/silent_file.txt
-d c:\\temp\\silent_file.txt -t text
```

7. Migrate the data collector using the silent response file:

```
tacmd executecommand -m System -c "migrate.bat -silent full_path_to_silent_file\\silent_file.txt"
-w path_to_DC_home\bin
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "migrate.bat -silent C:\\temp\\silent_file.txt"
-w C:\\IBM\\ITM\\dchome\\7.2.0.0.4\\bin
```

8. Restart the application server instances.
   a. Stop the application server.

```
tacmd executecommand -m System -c "stopServer.bat server_name" -w profile_home\bin
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "stopServer.bat server1"
-w C:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01\\bin
```

b. Start the application server:

```
tacmd executecommand -m System -c "startServer.bat server_name -w profile_home\bin"
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "startServer.bat server1"
-w C:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01\\bin
```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Enabling the ITCAM for SOA data collectors on the remote system

After you install the monitoring agent remotely on one or more managed systems, you must enable the ITCAM for SOA data collectors for the application server runtime environments that are being monitored on each remote system. To enable the data collectors, run the Data Collector Configuration utility or run the `KD4configDC` script as described in Part 4, "Configuring ITCAM for SOA-specific data collectors for runtime environments," on page 373.

The ITCAM for SOA data collector can be installed and configured remotely using the procedures in Part 4, "Configuring ITCAM for SOA-specific data collectors for runtime environments," on page 373.

Uninstalling IBM Tivoli Composite Application Manager for SOA on Windows systems

After you upgrade your Tivoli Monitoring environment, you cannot restore the environment to the previous level. If you uninstall Tivoli Monitoring after an upgrade, all of Tivoli Monitoring is removed, and any subsequent installation is equivalent to installing for the first time.

The same is true for ITCAM for SOA. After you upgrade your environment from a previous version of ITCAM for SOA to version 7.2 or later, there is no way to return to the previous version. If you uninstall ITCAM for SOA after an upgrade, all of ITCAM for SOA is removed, and any subsequent installation is equivalent to installing for the first time.

Tivoli Monitoring does not support uninstalling the ITCAM for SOA application support files from the Tivoli Monitoring environment. After you install the ITCAM for SOA application support files on a Tivoli Enterprise Portal, Tivoli Enterprise Portal Server or Tivoli Enterprise Monitoring Server computer, there is no way to remove these support files without completely uninstalling all of Tivoli Monitoring.

This also means that you cannot uninstall the SOA Domain Management Server or Tivoli Common Object Repository support from the Tivoli Enterprise Portal Server configuration, or remove it from the Tivoli Enterprise Portal Server computer.

To uninstall IBM Tivoli Composite Application Manager for SOA from your services environment, complete the tasks in the next sections.

Before uninstalling the monitoring agent

Before uninstalling the ITCAM for SOA monitoring agent, complete the following tasks:

1. If the system is currently running a Tivoli Enterprise Portal desktop or browser client, close it.
2. Open Manage Tivoli Enterprise Monitoring Services. If any of the following services are running, stop them. Right-clicking the services and selecting **Stop** from the menu):
   - The ITCAM for SOA monitoring agent
   - Tivoli Enterprise Portal Server
   - Tivoli Enterprise Monitoring Server
3. Close the Manage Tivoli Enterprise Monitoring Services utility.
4. If you have not done so, disable data collection for your runtime environments. Follow the procedures documented in Part 4, "Configuring ITCAM for SOA-specific data collectors for runtime environments," on page 373. You might have to stop affected application servers as part of the procedure.

   Beginning with ITCAM for SOA version 7.2, you no longer disable data collection for the ITCAM Data Collector for WebSphere by using the `ConfigDC` utility. Instead, use the ITCAM Data Collector for WebSphere Unconfiguration utility to disable data collection. For more information about unconfiguring the ITCAM Data Collector for WebSphere, see "Unconfiguring ITCAM Data Collector for WebSphere" on page 282.

   Beginning with ITCAM for SOA version 7.2 Fix Pack 1, you no longer disable data collection for WebSphere Message Broker environments by using the ITCAM for SOA `ConfigDC` utility. Instead, unconfigure Data Collector for Message Broker using the procedure in "Disabling data collection" on page 369.

   Restriction: If you are running BEA WebLogic Server application server environments, you do not have to stop this service now to perform the agent uninstallation. However, after uninstalling the agent, stop and restart the application server at a later time (for example, during off-shift hours).

Considerations for uninstalling the WebSphere Application Server data collector

If you are uninstalling the ITCAM for SOA version 7.2 monitoring agent because you want to reinstall the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector, you must not delete `KD4.dc.properties` properties file or the *`ITCAM4SOA_Home`*`\KD4` directory after uninstalling the data collector. Instead, navigate to the `\KD4\config` directory and manually remove the following properties from the `KD4.dc.properties` file before you uninstall the monitoring agent:

- `kd4.ira.supportsFile.service`
- `kd4.ira.supportsFile.staticBPM`
- `Kd4.ira.supportsFile.dynamicBPM`
- `kd4.ira.supportsFile.dynamicBPD`

Uninstalling the monitoring agent on Windows systems

To uninstall the monitoring agent, complete the following steps:

1. Select **Start** > **Control Panel** > **Add or Remove Programs**.
2. Double-click **IBM Tivoli Monitoring**.
3. Choose **Modify** and click **Next**.

4. Deselect the monitoring agent to uninstall it.
5. If you want to uninstall the Data Collector for WebSphere Message Broker, deselect it. You must disable data collection by removing `KK3UserExit` from all message flows and WebSphere Message Broker instances before you uninstall the data collector. For more information, see "Disabling data collection" on page 369.
6. The uninstallation wizard is started. Follow the on-screen prompts to complete the uninstallation.

Important: If the home directory of ITCAM Data Collector for WebSphere was specified to be outside of the IBM Tivoli Monitoring home directory, the data collector home directory is not removed during the uninstallation and must be removed manually.

Uninstalling ITCAM for SOA Tools

You might also have the ITCAM for SOA Tools (Web Services Navigator) installed on the local computer. This is shown as a separate entry in under Add or Remove Programs in the Control Panel. You can also uninstall the ITCAM for SOA Tools at this time, if applicable. For more information about uninstalling ITCAM for SOA Tools, see the *IBM Tivoli Composite Application Manager for SOA Tools*.

Removing tables from the warehouse database

You might still have a database installed if you configured historical data collection. The database is not deleted as part of this uninstall process because other IBM Tivoli monitoring agents might also be using it. Follow the procedures documented in your database software publications for removing any unwanted tables from the warehouse database.

Removing files and folders

When you uninstall ITCAM for SOA, navigate to the `\KD4\config` folder and either clear or delete the `KD4.dc.properties` file. If you do not clear or delete this properties file, and later install the monitoring agent again, the configuration settings for data collector control remain at the settings used for the previous installation, and not the default settings.

You must also delete the *`ITCAM4SOA_Home`*`\KD4` folder, where *ITCAM4SOA_Home* is the directory location where ITCAM for SOA is installed. See "The IBM Tivoli Composite Application Manager for SOA home directory" on page xvi for information about how to determine the value of *ITCAM4SOA_Home*.

Important: When you are uninstalling ITCAM for SOA version 7.2 because you want to reinstall the ITCAM for SOA 7.1.1 WebSphere Application Server Data Collector, do no clear or delete the `KD4.dc.properties` file or delete the *`ITCAM4SOA_Home`*`\KD4` folder. Instead, delete the properties specified in "Considerations for uninstalling the WebSphere Application Server data collector" on page 73 from the `KD4.dc.properties` file.

Removing SOA Domain Management Server and Tivoli Common Object Repository databases

The databases used with SOA Domain Management Server and Tivoli Common Object Repository are not deleted as part of the uninstallation process. Follow the procedures documented in your database application software publications for removing an unused database.

Installing and uninstalling language support

A Language Pack enables user interaction with the monitoring agent in a language other than English. For example, when a Spanish language pack is installed, the Tivoli Enterprise Portal Server workspaces and the internal messages of the monitoring agent are displayed in Spanish.

To enable full support for a language, you must install the language pack on the monitoring agent host and all hosts where the monitoring agent support files are installed (Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and all Tivoli Enterprise Portal desktop clients).

If you no longer want to use a language, uninstall the language pack for the language.

Remember: This procedure assumes that language support for the same language is installed on Tivoli Monitoring. If not, see the *IBM Tivoli Monitoring: Installation and Setup Guide* and install the base language support for Tivoli Monitoring before installing language support for the monitoring agent.

Installing a language pack on Windows systems

To install a language pack, first make sure that you have installed the product in English, then perform the following steps:

1. Double-click `lpinstaller.bat` on the language pack installation image to start the installation program.
2. Select the language of the installer and click **OK**.
   In this step, you select the language for the installer user interface, not the language pack that will be installed.
3. Click **Next** on the Introduction panel.
4. Click **Add/Update** and click **Next**.
5. Select the folder in which the National Language Support package (NLSPKG) files are located.

   Tip: Typically the NLSPKG files are in the `nlspackage` folder where the installer executable is located.
6. Select the agent for which you want to process national language support and click **Next**.
7. Select the languages that you want to install and click **Next**.

   Tip: You can hold down the **Ctrl** key for multiple selections.
8. Examine the installation summary page and click **Next** to begin installation.
9. Click **Done** after installation completes to exit the installer.
10. Start the **Manage Tivoli Enterprise Monitoring Services** utility and restart Tivoli Enterprise Portal Desktop Client and Tivoli Enterprise Portal Server, if a language pack was installed for either of these components. If the Eclipse Help Server is running, restart it as well.

Uninstalling language packs

Perform these steps to remove the language packs for agents:

1. From the language pack installation image, double click `lpinstaller.bat`.
2. Select the language of the installer and click **OK**.

Important: In this step, you select the language for the installer user interface, not the language pack that is to be installed.

3. On the introduction window, click **Next**.
4. Select **Remove** and click **Next**.
5. Select the agent for which you wish to remove national language support and click **Next**.
6. Select the languages to uninstall and click **Next**.

   Tip: To select multiple languages at the same time, you can hold down the **Ctrl** key and select the languages that you want.
7. Examine the uninstallation summary page. To begin the uninstallation, click **Next**.
8. To exit the installer, click **Done**.
9. If you are uninstalling a language pack from Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart Tivoli Enterprise Portal Server and Tivoli Enterprise Portal desktop client. If the Eclipse Help Server is running, restart it as well.

Chapter 3. Installing ITCAM for SOA on Linux and UNIX systems

Before you install ITCAM for SOA version 7.2 Fix Pack 1, refer to "Performing a pristine installation of ITCAM for SOA version 7.2 Fix Pack 1" on page 19 for the ITCAM for SOA installation prerequisites and for the roadmap of installation tasks.

Before you upgrade to ITCAM for SOA version 7.2, refer to "Upgrading to ITCAM for SOA version 7.2" on page 23 for the ITCAM for SOA upgrade prerequisites and for the roadmap of upgrade tasks.

Before you update to ITCAM for SOA version 7.2 Fix Pack 1, refer to "Updating to ITCAM for SOA version 7.2.0.1" on page 28 for the ITCAM for SOA update prerequisites and for the roadmap of update tasks.

Remember: ITCAM for SOA supports only a single installation per computer system.

Enabling application support on the monitoring server, portal server, and desktop client

To ensure the monitoring agent works within your Tivoli Monitoring infrastructure, application support files that are provided with the installation of the ITCAM for SOA agent must be distributed to the Tivoli Monitoring components.

Application support files are provided with the installation of the ITCAM for SOA agent.

Application support files are automatically installed and enabled on the monitoring server without the need to recycle the monitoring server if you are integrating with Tivoli Monitoring version 6.2.3 or later and the Tivoli Monitoring components and the agent are enabled for self-description. The conditions that must be met for self-description to operate are specified in "Enabling application support through self-description" on page 36. Application support files must be manually installed on the portal server and the portal client.

If the agent and the Tivoli Monitoring components are not enabled for self-description, you must manually install application support files on the Tivoli Monitoring components. For more information, see "Installing and enabling application support manually before installing the agent" on page 78.

Enabling application support through self-description

Tivoli Monitoring version 6.2.3 or later agents, which are enabled for self-description, install application support files and enable application support on the IBM Tivoli Monitoring infrastructure automatically. ITCAM for SOA is enabled by default for self-description. When the ITCAM for SOA agent is installed, and the hub and remote monitoring servers are enabled for self-description, application support files are automatically installed on the hub monitoring server and the remote monitoring server, without the need to recycle the monitoring server.

Application support files must be installed manually on portal server and the portal client. ITCAM for SOA requires that configuration of topology support for SOA Domain Management Server and Tivoli Common Object Repository on the portal server be performed manually.

Although the self-describing agent is enabled by default for ITCAM for SOA, a number of conditions apply:

- All Tivoli Management Services server components must be at version 6.2.3 or later.
- The agent framework must be at version 6.2.3 or later.

In ITCAM for SOA version 7.2, agent framework version 6.2.2 is installed a part of an install or upgrade of ITCAM for SOA. However, if you install another IBM Tivoli Monitoring agent, such as an OS agent, and its agent framework is at version 6.2.3, its installation might upgrade the agent framework of ITCAM for SOA to version 6.2.3.

Remember: Not all OS agents running version 6.2.3, which share the same IBM Tivoli Monitoring home directory as ITCAM for SOA, upgrade the agent framework to version 6.2.3. You must verify that the agent framework has been upgraded to version 6.2.3 before using self-description for ITCAM for SOA.

To identify the agent framework version after you install or upgrade ITCAM for SOA, complete the following steps:

1. From the command prompt, navigate to *ITM_home*/bin directory.
2. Run the following command:
   ```
   ./cinfo -t
   ```
3. Locate the line for the agent framework in the output and note the version. For example:
   ```
   ax IBM Tivoli Monitoring Shared Libraries li6263 06.22.02.00
   d0126a 20120716 1412
   ```

You must verify that these conditions are met before you can use self-description for deploying application support to the monitoring server.

When the self-describing application update is complete, and the application support files are manually installed on the portal server, you should see the following new agent data in the portal client:

- Historical Configuration is updated with any new attributes
- Workspaces are updated
- New or updated situations, policies and take actions
- Queries are updated
- Help server files are updated

The self-describing agent feature is disabled by default on the hub monitoring server. The procedure for enabling self-description on the hub monitoring server is documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing and enabling application support manually before installing the agent

Enabling application support is sometimes referred to as adding or activating application support.

Multiple versions of ITCAM for SOA can be integrated with Tivoli Monitoring. If self-description is not enabled, you must install application support files from the agent that is at the latest version. For example, if your environment has ITCAM for SOA versions 7.2 and 7.1.1, ensure you install the application support files for the latest version, in this case version 7.2.

When all of the Tivoli Monitoring components are installed on the same computer system, application support files for each of the monitoring components must be installed at the same time.

When you install application support on your Tivoli Enterprise Monitoring Server, you must be logged in as the user who installed the Tivoli Enterprise Monitoring Server.

The Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal must be stopped before you install the application support files.

To install application support for the ITCAM for SOA agent, complete these steps:

1. Close the Manage Tivoli Enterprise Monitoring Services utility if it is open.
2. Mount the ITCAM for SOA installation media at the location you choose for the local system, following the standard procedures for the operating system.
3. From the root directory of the installation media, enter the following command to start the installation program `./install.sh`
4. When prompted for the Tivoli Monitoring home directory, press Enter to accept the default (`/opt/IBM/ITM`) or type the full path to the installation directory that you used. You are presented with the prompt `Ok to use`. Enter 1 and press Enter to confirm that the specified home directory can be used.
5. The following prompt is displayed:
   ```
   Select one of the following:
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS).
   3) Install TEMS support for remote seeding
   4) Exit install.
   Please enter a valid number:
   ```
6. Type 1 to start the installation and press Enter.
7. The software license agreement is displayed after the initialization. Enter 1 to accept the agreement and press Enter.
8. A numbered list of available operating systems and installation components is displayed:
   ```
   Product packages are available for the following operating systems and
   component support categories:
    1) IBM Tivoli Monitoring components for this operating system
    2) Tivoli Enterprise Portal Browser Client support
    3) Tivoli Enterprise Portal Desktop Client support
    4) Tivoli Enterprise Portal Server support
    5) Tivoli Enterprise Monitoring Server support
    6) Other operating systems
   ```
9. Type 5 to install application support for the monitoring server and press Enter.
10. Type 1 to confirm and press Enter.
11. The list of the components that are available for the installation of application support for the monitoring server is displayed. For example:

```
The following application supports are available for installation:

1) IBM Tivoli Composite Application Manager for SOA V07.20.01.00
2) all of the above.
```

12. Enter the number that represents all components and press Enter.
13. Type 1 to confirm the installation of application support for the monitoring server. The installation begins.
14. When all of the components are installed, you are asked whether you want to install additional products or product support packages. For example,

    ```
    Do you want to install additional products or product support
    packages [ 1=Yes, 2=No ; default is "2" ] ?
    ```

    Enter 1 to install application support for additional components.
15. The numbered list of available installation components is displayed. Type 4 to install application support for the portal server and press Enter.
16. Type 1 to confirm and press Enter.
17. The list of the components that are available for the installation of application support for the portal server is displayed.
18. Enter the number that represents all components and press Enter.
19. Type 1 to confirm the installation of application support for the portal server. The installation begins.
20. When all of the components are installed, you are prompted to install components for a different operating system.
    Enter 1 to install application support for additional components.
21. The numbered list of available operating systems and installation components is displayed. Type 2 to install application support for the browser client or type 3 to install application support for the desktop client and press Enter.
22. Type 1 to confirm and press Enter.
23. The list of the components available for the installation of application support for the browser is displayed.
24. Enter the number that represents all components and press Enter.
25. Type 1 to confirm the installation of application support for the portal server. The installation begins.
26. When all of the components are installed, you are prompted to install components for a different operating system. Type 2 to confirm that no additional components are to be installed and press Enter.
27. When the installation program completes, you see a message that indicates that the application support files are installed:

    ```
    Following Tivoli Enterprise Monitoring Server product support were installed:
      *) ITCAM for SOA
    Note: This operation causes the monitoring server to restart.
    ```
28. You are prompted to add the default managed system groups when you process the application-support files:

    ```
    Choose one of the following options to add or update the situation
    distribution definition to include the default managed
    system groups:

     1) ALL - This option adds the default managed
    system groups to all the applicable situations.
    Note that not all situations have the
    default managed group setting. For some,
    you might need to manually define the distribution in the Tivoli
    ```

```
Enterprise Portal due to the specific content
 of the agent support package.
 2) NONE - The default managed system group is not added to any situation.
```

The *All* selection provides an option to add the default managed systems group to all applicable situations. Enter 1 to add the default managed system groups to all applicable situations and press Enter.

29. The installation program completes the installation and exits.
30. Reconfigure the portal server and the browser client to enable application support. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd config -A cq
    ```

    At any prompts, press Enter to accept the default values.
31. Restart the portal server. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd agent start cq
    ```
32. Reconfigure the desktop client to enable application support. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd config –A cj
    ```

    At any prompts, press Enter to accept the default values.
33. Start the desktop client. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd agent start cj
    ```
34. Start the monitoring server. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd server start tems_name
    ```
35. Activate application support on the monitoring server. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd support -t tems_name d4
    ```
36. Stop the monitoring server. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd server stop tems_name
    ```
37. Start the monitoring server to enable application support. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd server start tems_name
    ```

Installing, upgrading, and updating the monitoring agents and data collectors

This procedure installs or upgrades the agent on each computer system where one or more of the supported application server runtime environments (for example, IBM WebSphere Application Server) are installed. For a DataPower environment, the agent is installed on the computer system where the DataPower proxy is located.

Installing the monitoring agent and the data collectors

The agent consists of the monitoring agent and the data collector components. A data collector intercepts request and response messages of the services that you are monitoring. The monitoring agent collects the information from the data collector, and transfers the information to the monitoring server for presentation and storage. In ITCAM for SOA version 7.2, there are two types of data collectors:

- ITCAM for SOA data collectors, installed automatically as part of the installation of the monitoring agent and used to configure data collection for all runtime environments, apart from the WebSphere Application Server and WebSphere Message Broker environments.
- The ITCAM Data Collector for WebSphere, used to configure data collection for WebSphere application server instances

In ITCAM for SOA version 7.2 Fix Pack 1, the Data Collector for WebSphere Message Broker is introduced to configure data collection for WebSphere Message Broker environments

Before ITCAM for SOA version 7.2, both the data collector components and the monitoring agent component were installed or upgraded as part of the installation or upgrade of the monitoring agent. In ITCAM for SOA version 7.2 and later, the ITCAM Data Collector for WebSphere is installed after the monitoring agent is installed in a location that you specify.

After the monitoring agent installation completes, the installer automatically launches the Data Collector Configuration Utility for enabling data collection in the supported runtime environments. For all data collectors, apart from the ITCAM Data Collector for WebSphere, as soon as the Data Collector Configuration utility launches, the installation of the data collector is complete, and you can enable data collection with this utility. Alternatively, you can exit this utility and use the `KD4ConfigDC` script to configure the data collector.

Installing and configuring the ITCAM Data Collector for WebSphere

Beginning with ITCAM for SOA version 7.2, the ITCAM Data Collector for WebSphere is a new component that is shared with the following components and products:

- ITCAM for SOA
- ITCAM Agent for WebSphere Applications
- ITCAM for WebSphere Application Server
- IBM Application Performance Diagnostics Lite
- ITCAM for Transactions

Because this data collector component was not in version 7.1.1, when you are upgrading from version 7.1.1, you must install it in a location that you specify before you enable the data collector. The data collector must be configured using the new ITCAM Data Collector for WebSphere Configuration utility command-line utility.

When the installation, upgrade, or update of the monitoring agent completes, the `ConfigDC` utility is started. When you select the option to configure the WebSphere Application Server, a command-line window opens and you are prompted to specify the data collector home directory. Next, the data collector is installed in the specified directory. If the same version, release, and maintenance level of the data collector is already installed in the directory, the data collector is not reinstalled.

The ITCAM Data Collector for WebSphere Configuration utility for configuring the data collector is started in console mode. You must integrate the data collector with the ITCAM for SOA monitoring agent with this utility.

Considerations for the installation or upgrade of the monitoring agent and data collectors

This installation of the monitoring agent and data collectors is based on the following assumptions:

- You installed or upgraded your Tivoli Monitoring environment to one of the minimum supported levels (see "Software and hardware prerequisites" on page 15).
- As part of the process of installing or upgrading your Tivoli Monitoring environment, you installed and configured one or more supported database applications (IBM DB2, Microsoft SQL Server, or Oracle). The database application is used for storing historical data or for viewing service registry, business process, or service-to-service topology data in your Tivoli Monitoring workspaces. For database information, see "Databases" on page 13.
- You installed or upgraded application support for the Tivoli Monitoring components. For more information about installing application support, see "Enabling application support on the monitoring server, portal server, and desktop client" on page 77. If your IBM Tivoli Monitoring components are installed on the same computer systems as your application server runtime environment, application support can be installed during the installation of the monitoring agent.

Permissions for installing, upgrading, or updating the monitoring agent

If you have multiple Tivoli Monitoring components (including multiple monitoring agents) installed on the same computer, you should install all of the agents using the same user. (The only exception is the portal server which must be installed as root.)

If you do not want to install Tivoli Monitoring components, including the monitoring agents, as root on Linux and UNIX, create a user on the computer where you plan to install the Tivoli Monitoring components and use it to install all Tivoli Monitoring-related components (except the portal server) on that computer. For more information about creating the non-root user, see the *Create an IBM Tivoli account for installing and maintaining the installation directory* section of the *IBM Tivoli Monitoring: Installation and Setup Guide*.

To install the ITCAM for SOA monitoring agent as a non-root user on Linux and UNIX systems, complete the following steps:

1. Install the ITCAM for SOA monitoring agent.
2. Copy the `KD4BaseDirConfig.properties` from the `ITM_home/platform/d4/KD4/config` directory to the `/etc` directory after the installation completes. This step might require your user to have root authority.
3. Change the file permissions for the monitoring agent using the instructions in "Changing the file permissions for agents" on page 94. These instructions direct you to create a group (for example, itmusers) that owns all of the IBM Tivoli Monitoring component files on the computer system.

For information about the permissions that are required to configure data collection for the ITCAM Data Collector for WebSphere, see "Permissions needed to configure for data collection" on page 376.

Before installing or upgrading the monitoring agent

Complete the following tasks before you install or upgrade the monitoring agent.

Before installing the monitoring agent

Before you run the installation program, complete the following steps:

1. Close the Manage Tivoli Enterprise Monitoring Services utility if it is open on the application server where you are installing the monitoring agent.
2. If the BEA WebLogic Server is running on the same computer system where you are installing the monitoring agent, stop the server.

Before upgrading or updating the monitoring agent

Before installing over an existing installation, complete the following steps:

1. Close the Manage Tivoli Enterprise Monitoring Services utility if it is open on the application server where you are installing the monitoring agent.
2. Stop all application servers on the computer where the monitoring agent is being installed.
3. If you have a DataPower data collector proxy that is running on this computer system, stop the data collector.
4. Disable any existing ITCAM for SOA data collectors on this computer system. (For the version-specific procedures for disabling each data collector, see the ITCAM for SOA data collector chapters in Part 4, "Configuring ITCAM for SOA-specific data collectors for runtime environments," on page 373.)

Installing, upgrading, or updating the monitoring agent

To install, upgrade, or update ITCAM for SOA on a supported Linux and UNIX operating system, complete the following steps on each Linux or UNIX computer system where you plan to monitor services. See the Tivoli Monitoring documentation for general procedures for installing monitoring agents on these operating systems. If you are installing, upgrading, or updating a monitoring agent on a computer system where Tivoli Monitoring components are already installed, you must also install application support files as part of the installation procedure.

Tip:

- In the installation process, if you are upgrading to ITCAM for SOA version 7.2, the ITCAM for SOA monitoring agent is displayed as `IBM Tivoli Composite Application Manager for SOA  V07.20.00.00`.
- If you are installing or updating to ITCAM for SOA version 7.2 Fix Pack 1, the ITCAM for SOA monitoring agent is displayed as `IBM Tivoli Composite Application Manager for SOA  V07.20.01.00`.

1. Mount the ITCAM for SOA installation media at the location you choose for the local system, following the standard procedures for your operating system.
2. From the root directory of the installation media, enter the following command to start the installation program: `./install.sh`
3. When prompted for the Tivoli Monitoring home directory, press Enter to accept the default (`/opt/IBM/ITM`) or type the full path to the installation directory that you used. Type 1 and press Enter when you see `OK to use it`.

   Remember: If you are installing over an existing installation, you must use the existing installation directory.
4. The following prompt is displayed:

```
Select one of the following:
1) Install products to the local host.
2) Install products to depot for remote deployment (requires TEMS).
3) Install TEMS support for remote seeding
4) Exit install.
Please enter a valid number:
```

5. Type 1 to start the installation and press Enter.
6. The software license agreement is displayed after the initialization. Enter 1 to accept the agreement and press Enter.
7. If you are performing a pristine installation on a system where no Tivoli Monitoring components are installed, you are prompted to type a 32 character key for encrypting your Secure Socket Layer (SSL) connections with Tivoli Enterprise Monitoring Server to protect sensitive data that is being transmitted. This key must be the same key that is specified during the installation of the Tivoli Enterprise Monitoring Server to which this monitoring agent connects.
8. If you are upgrading, you are prompted with a list of prerequisites to install. Enter 1 to install these prerequisites:

   ```
   Do you want to install these prerequisites [ 1=Yes, 2=No ; default is "1" ] ?1
   ```

9. A numbered list of available operating systems is displayed:

   ```
   Product packages are available for this operating system and
   component support categories:

    1) IBM Tivoli Monitoring components for this operating system
    2) Tivoli Enterprise Portal Browser Client support
    3) Tivoli Enterprise Portal Desktop Client support
    4) Tivoli Enterprise Portal Server support
    5) Tivoli Enterprise Monitoring Server support
    6) Other operating systems
   Type the number or type "q" to quit selection
   ```

10. Type 1 and press Enter.
11. Type 1 to confirm and press Enter.
12. A numbered list of available agents is displayed.

    When you install on a supported Linux x86-64 operating system, you select either the `ITCAM for SOA V07.20.00.00 for Linux AMD64 R2.6 (64 bit)` or `ITCAM for SOA V07.20.01.00 for Linux AMD64 R2.6 (64 bit)` option. The version you select depends on whether you are upgrading to version 7.2 or you are installing or upgrading to version 7.2 Fix Pack 1 of ITCAM for SOA.

    Find the IBM Tivoli Composite Application Manager for SOA agent and type the corresponding number and press Enter.
13. You are asked to confirm your selection. For example:

    ```
    The following products will be installed:

     IBM Tivoli Composite Application Manager for SOA V07.20.01.00

    Are you selections correct [1=Yes, 2=No ; default is "1"]
    ```

    Type 1 to confirm your selection.
14. If the installer detects that the same version of the ITCAM for SOA agent exists on the computer system, it prompts you to confirm that you want to replace it.
15. The installation begins. A progress message is displayed while the agent is being installed. For example:

    ```
    ... installing "IBM Tivoli Composite Application Manager for SOA
    V07.20.01.00..."
    ```

16. When all of the components are installed, you are asked if you want to install additional products or application support files:

    ```
    Do you want to install additional products or product support packages
    [ 1=Yes, 2=No ; default is "2" ] ?
    ```

17. If you want to install the Data Collector for WebSphere Message Broker, type 1. Otherwise, accept the default response of 2, press Enter, and skip to step 24.

    Before you install the data collector, verify that the data collector is not already installed as part of ITCAM for Transactions.

    - If the data collector is already installed as part of ITCAM for Transactions and is at the same maintenance level, skip the steps to install and enable the data collector. Instead, integrate the data collector with the ITCAM for SOA monitoring agent by setting the `default.kd4.enabled` property in the `KK3.dc.properites` file to `true`. For more information about integrating the data collector with ITCAM for SOA, see "Integrating the data collector with ITCAM for SOA and ITCAM for Transactions" on page 368.
    - If the data collector is installed but is at an earlier maintenance level, install the data collector and follow the procedure for updating the maintenance level of the data collector in "Upgrading to the Data Collector for WebSphere Message Broker" on page 360.
    - If an older version of the data collector is installed, follow the upgrade procedure in "Upgrading to the Data Collector for WebSphere Message Broker" on page 360.

18. A numbered list of agents and components is displayed.

    Find the Data Collector for WebSphere Message Broker component and type the corresponding number and press Enter.

19. You are asked to confirm your selection. For example:

    ```
    The following products will be installed:

     Data Collector for WebSphere Message Broker V07.40.00.00

    Are you selections correct [1=Yes, 2=No ; default is "1"]
    ```

    Type 1 to confirm your selection.

20. If the installer detects that the same version of the Data Collector for WebSphere Message Broker exists on the computer system, it prompts you to confirm that you want to replace it.

21. The installation begins. A progress message is displayed while the data collector is being installed:

    ```
    ... installing "Data Collector for WebSphere Message Broker
    V07.40.00.00..."
    ```

22. When the data collector is installed, you are asked if you want to install additional products or application support files:

23.
    ```
    Do you want to install additional products or product support packages
    [ 1=Yes, 2=No ; default is "2" ] ?
    ```

24. If you are installing application support files as part of your installation of the monitoring agent, type 1. Otherwise, accept the default response of 2, press Enter, and skip to step 46 on page 88.

25. The numbered list of available operating systems and installation components is displayed. Select the option to install application support for the monitoring server and press Enter.

26. Type 1 to confirm and press Enter.

27. The list of the components that are available for the installation of application support for the monitoring server is displayed. For example:

```
The following application supports are available for installation:

1) IBM Tivoli Composite Application Manager for SOA V07.20.01.00
2) all of the above.
```

28. Enter the number that represents all components and press Enter.
29. Type 1 to confirm the installation of application support for the monitoring server. The installation begins.
30. When all of the components are installed, you are asked whether you want to install components for a different operating system. For example:

    ```
    Do you want to install additional products or product
    support packages [ 1=Yes, 2=No ; deafult is "2" ] ?
    ```

    Enter 1 to install application support for additional components.
31. The numbered list of available operating systems and installation components is displayed. Select the option to install application support for the portal server and press Enter.
32. Type 1 to confirm and press Enter.
33. The list of the components that are available for the installation of application support for the portal server is displayed.
34. Enter the number that represents all components and press Enter.
35. Type 1 to confirm the installation of application support for the portal server. The installation begins.
36. When all of the components are installed, you are prompted to install components for a different operating system.
    Enter 1 to install application support for additional components.
37. The numbered list of available operating systems and installation components is displayed. Type 2 to install application support for the browser client or type 3 to install application support for the desktop client and press Enter.
38. Type 1 to confirm and press Enter.
39. The list of the components available for the installation of application support for the browser or desktop client is displayed.
40. Enter the number that represents all components and press Enter.
41. Type 1 to confirm the installation of application support for the portal server. The installation begins.
42. When all of the components are installed, you are prompted to install components for a different operating system. Type 2 to confirm that no additional components are to be installed and press Enter.
43. When the installation program completes, you see a message that indicates that the application support files are installed:

    ```
    Following Tivoli Enterprise Monitoring Server product support were installed:
      *) ITCAM for SOA
    Note: This operation causes the monitoring server to restart.
    ```

44. You are asked whether you want to seed application support on the Tivoli Enterprise Monitoring Server:

    ```
    Do you want to seed product support on the Tivoli Enterprise Monitoring Server?
     [ 1=Yes, 2=No ; default is "1" ] ?
    ```

    Enter 1 to automatically seed the monitoring agent with the monitoring server.
45. If you are installing application support files as part of the installation or upgrade of the agent, you are prompted to add the default managed system groups to monitoring agents situations:

```
Choose one of the following options to add or update the situation
distribution definition to include the default
managed system groups:

 1) ALL - This option adds the default managed system groups to all
the applicable situations. Note that not all situations have
 the default managed group setting. For some, you
might need to manually define the distribution in the Tivoli
 Enterprise Portal due to the specific content
of the agent support package.
 2) NONE - The default managed system group is not added to any situation.
```

The All selection provides an option to add the default managed system groups to all applicable situations. Enter 1 to add the default managed system groups to all applicable situations and press Enter.

46. The installation program completes the installation and exits.
47. The installer detects that some additional procedures might have to be performed and presents a message that indicates that a data collector might have to be installed and configured.

```
Installation step complete.
Installer has found additional procedures for following products:
 *)  ITCAM for SOA

These procedures will be run now.

Calling exit point for ITCAM for SOA:
```

48. The Data Collector Configuration utility automatically starts in console mode to configure your data collector and prompts you to select a language to use for the Data Collector Configuration utility:

```
Select a language to be used for this wizard.

[X] 1  - English
[ ] 2  - French
[ ] 3  - German
[ ] 4  - Italian
[ ] 5  - Japanese
[ ] 6  - Korean
[ ] 7  - Portuguese (Brazil)
[ ] 8  - Simplified Chinese
[ ] 9  - Spanish
[ ] 10 - Traditional Chinese

To select an item enter its number, or 0 when you are finished: [0]
```

Enter the number that represents the language to use and selected Enter.

49. The Data Collector Configuration utility welcome window is displayed:

```
Data Collector Configuration Utility - InstallShield Wizard - Console Mode

Welcome to the InstallShield Wizard for the Data Collector Configuration
Utility. The Data Collector Configuration Utility helps you to enable or
disable data collection in your supported runtime environments. To continue,
choose Next.
Data Collector Configuration Utility
IBM
http://www.ibm.com


Press 1 for Next, 3 to Cancel or 5 to Redisplay [1]
```

50. Enter 1 to proceed to the next step. The list of runtime environments for which data collection can be configured are displayed:

```
Data Collector Configuration Utility - InstallShield Wizard - Console Mode

   1. IBM WebSphere Application Server
   3. BEA WebLogic Server
   4. JBoss
   5. SAP NetWeaver
   6. WebSphere Message Broker
   7. Configure Transaction Tracking settings
   8. DataPower SOA Appliance
   9. WebSphere Community Edition

   10. Exit the Data Collector Configuration Utility.

Select the runtime environment to enable or disable for data collection: 1

Press 1 for Next, 3 to Cancel or 5 to Redisplay [1]
```

Tip: You cannot configure Data Collector for WebSphere Message Broker with this utility. The option `WebSphere Message Broker` is provided for disabling a previous version of the WebSphere Message Broker data collector.

51. If you are upgrading to ITCAM for SOA 7.2, or you want to postpone the configuration of data collectors, you can enter 2 to cancel and skip to step "Verify completion of installation procedure" on page 91 to complete the installation task.

    If you are updating to ITCAM for SOA version 7.2 Fix Pack 1 and you are configuring data collection for a WebSphere Application Server environment, enter 1 to install and configure the ITCAM Data Collector for Websphere and press Enter.

    The ITCAM Data Collector for WebSphere in ITCAM for SOA version 7.2 and later is a component that is shared with the following products:

    - ITCAM Agent for WebSphere Applications version 7.2
    - ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5
    - IBM Application Performance Diagnostics Lite
    - ITCAM for Transactions

    If ITCAM Agent for WebSphere Applications version 7.2 is already installed under the *ITM_home* directory or if you are performing a reinstallation, the same version, release, and maintenance level of the ITCAM Data Collector for WebSphere might be installed under *ITM_home*. If the installer detects that the ITCAM Data Collector for WebSphere is already installed under *ITM_home*, the installation of the data collector is skipped and the data collector configuration utility is displayed. Skip to step "Step 19: Configure the ITCAM Data Collector for WebSphere" on page 56.

    Remember: The same version, release, and maintenance level of ITCAM Data Collector for WebSphere might be installed and configured for the same WebSphere profile, but the data collector installation might not be under the *ITM_home* directory:

    - If the data collector is installed by WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 or Application Performance Diagnostics Lite, the data collector installation is outside of the *ITM_home* directory. The installer does not detect that the data collector already exists. When prompted, you must specify the location of the data collector installation.

- If the data collector is installed by ITCAM Agent for WebSphere Applications version 7.2 outside of *ITM_home*, the installer does not detect that the data collector exists. When prompted, you must specify the location of the data collector installation.

52. When the same version, release, and maintenance level of the data collector is not already installed under the *ITM_home* directory, the installer opens a command prompt window.

    The installer prompts you to specify whether you want to:

    - Install the data collector in the `DC_home` directory (default install)
    - Reuse an existing data collector home directory (custom install)
    - Create a new data collector home directory (custom install)

    ```
    Choose the type of install to perform.
          1. default install
          2. custom install
    [default is: 1]:
    ```

    Enter 1 to install the data collector in the *DC_home* directory.

    Otherwise, enter 2 and specify the location of the data collector home directory. If the installer finds that the data collector home directory does not exist, it asks you whether you want to create the directory.

    ```
    Directory /opt/IBM/ITM/dchome/7.2.0.0.4 does not exist.  Is it ok to create?
    [1 - YES, 2 - NO]
    ```

    Enter 1 to create the directory. If you enter 2, you can enter a different data collector home directory or exit the command prompt.

    Restriction: You must not install the data collector in the same directory where version 7.1.1 of the ITCAM for SOA WebSphere Application Server data collector is installed.

    If the data collector installation does not already exist, the installer starts the installation of the data collector.

53. The installer starts the ITCAM Data Collector for WebSphere Configuration utility.

    If you are configuring the data collector only for an ITCAM for SOA environment, you must integrate the data collector at least with ITCAM for SOA, and optionally, integrate the data collector with ITCAM for Transactions. For description of the steps to follow when configuring the data collector with the ITCAM Data Collector for WebSphere Configuration utility, see "Configuring ITCAM Data Collector for WebSphere" on page 274.

    If you are installing ITCAM for SOA and you want to postpone the configuration of the ITCAM Data Collector for WebSphere until later, you can exit the utility. At a later time, use the ITCAM Data Collector for WebSphere Configuration utility to configure the data collector.

    If the data collector component of an older version of any of the following products is configured within the same profile, exit the utility, and migrate the data collector:

    - Older versions of the ITCAM Agent for WebSphere Applications, including:
      - ITCAM Agent for WebSphere Applications version 7.1
      - ITCAM for WebSphere version 6.1.0.4 or later
      - WebSphere Data Collector version 6.1.0.4 or later component of ITCAM for Web Resources version 6.2.0.4 or later
    - ITCAM for WebSphere Application Server version 7.2

For the migration procedure, see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291.

If an older version of ITCAM for SOA is configured for the same profile, exit the utility, and migrate the data collector (see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291).

If an earlier maintenance level of the ITCAM Data Collector for WebSphere is configured for the same profile, exit the utility, and migrate the data collector (see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291.

For a description of considerations when you install and configure IBM Business Process Monitoring considerations, an overview of installation and upgrade scenarios, and procedures for running the configuration utilities in interactive and silent modes, see Chapter 7, "Configuring data collection: WebSphere Application Server," on page 257.

Verify completion of installation procedure

When you complete the configuration of the data collectors and exit the Data Collector Configuration utility, you see a message to indicate that the additional data collector configuration procedure completed successfully:

```
Installation step complete.
Exit points procedures for following agents were executed:
  *) ITCAM for SOA    [Success]

You may now configure any locally installed IBM Tivoli Monitoring agent via the
"/opt/IBM/ITM_test/bin/itmcmd config" command.
```

You see this message only if the Data Collector Configuration utility was started automatically following the installation of the monitoring agent. When the installation of the monitoring agents and data collectors is complete, the installer prompts you to secure your IBM Tivoli Monitoring environment, if you have not already done so:

```
Do you want to secure this IBM Tivoli Monitoring installation
[ 1-yes, 2-no; "2" is default ]?
```

The product installation process creates most directories and files with world write permissions. IBM Tivoli Monitoring provides the `secureMain` utility to help you keep the monitoring environment secure. You can secure your installation now, or you can manually run the `secureMain` utility later. For more information about securing you IBM Tivoli Monitoring installation, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Enter `1` to secure the installation or `2` to defer until later.

If you installed application support files as part of the installation of the agent, reconfigure the portal server and browser client to enable application support:

1. Reconfigure the portal server and the browser client to enable application support. Run the following command from the *ITM_HOME*/`bin` directory:

   ```
   ./itmcmd config -A cq
   ```

   At any prompts, press Enter to accept the default values.
2. Restart the portal server. Run the following command from the *ITM_HOME*/`bin` directory:

   ```
   ./itmcmd agent start cq
   ```
3. Reconfigure the desktop client to enable application support. Run the following command from the *ITM_HOME*/`bin` directory:

```
./itmcmd config –A cj
```

At any prompts, press Enter to accept the default values.

4. Restart the desktop client. Run the following command from the *ITM_HOME*/bin directory:

   ```
   ./itmcmd agent start cj
   ```

The monitoring agent and data collectors are installed. You must also complete the tasks that are specified in the "Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1" on page 20, such as configuring topology support, reconfiguring and restarting the portal server, and enabling data collection, to complete the installation of the ITCAM for SOA agent.

Preparing the Tivoli Enterprise Portal browser client

After you install or upgrade the ITCAM for SOA monitoring agent, the user interface might not display properly when you view it from a Tivoli Enterprise Portal browser client. Before starting the Tivoli Enterprise Portal, you must clear the cache of your web browser and your IBM Java plug-in. To clear the cache, complete the following steps:

1. From your browser client, clear all temporary files, cookies, and history files.
2. To clear the Java plug-in, complete the following steps:
   a. Double-click **IBM Control Panel for Java** to launch the Java control program.
   b. On the **General** tab, click **Settings** in the **Temporary Internet Files** section.
   c. On the **Temporary Files Settings** dialog, click **Delete Files**.
   d. Click **OK** to close the Java control panel.

Additional procedure for Security Enhanced Linux (SELinux)

After installing ITCAM Data Collector for WebSphere on SELinux, for example, Red Hat Enterprise Linux Version 5 or SUSE Linux Enterprise Server Version 11, you must complete an additional procedure to identify the data collector shared libraries.

To identify the data collector shared libraries on SELinux, run the following command as root, substituting the installation directory for *DC_home* and the Tivoli Monitoring architecture identifier for *DC_architecture_code*:

```
chcon -R -t texrel_shlib_t

DC_home/toolkit/lib/DC_architecture_code
```

For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.

The architecture code identifiers for Linux systems are:

- `li6263`: Linux Intel R2.6 (32 bit)
- `lx8266`: Linux x86_64 R2.6 (64 bit)
- `lpp263`: Linux ppc R2.6 (32 bit)
- `lpp266`: Linux ppc R2.6 (64 bit)
- `ls3263`: Linux S390 R2.6 (32 bit)
- `ls3266`: Linux S390 R2.6 (64 bit)

For 64-bit systems, you must run the command twice to identify shared libraries for both 32-bit and 64-bit versions of the data collector.

(Optional) Additional procedure for Linux on Intel systems and Linux on System z systems

During an update from ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1 on Linux Intel systems and Linux System z systems, some backup files are created by the installer. The backup files are a result of platform code changes in ITCAM for SOA version 7.2 Fix Pack 1. Optionally, you can remove the backup files after you verify that the update completed successfully.

In ITCAM for SOA version 7.2, the platform code for ITCAM for SOA Linux Intel systems is `li6243`. The platform code in ITCAM for SOA version 7.2 Fix Pack 1 is `li6263`.

In ITCAM for SOA version 7.2, the platform code for ITCAM for SOA Linux System z systems is `ls3243`. The platform code in ITCAM for SOA version 7.2 Fix Pack 1 is `ls3263`.

As part of an update to ITCAM for SOA version 7.2 Fix Pack 1, a backup is created of the *ITM_home*/<*old_platform_code*>/d4 directory. The file d4<*old_platform_code*>.ver in the *ITM_home*/registry/ directory is renamed d4<*old_platform_code*>.dep.

Following an update to ITCAM for SOA version 7.2 Fix Pack 1, optionally complete the following steps:

1. Verify that the update to version 7.2 Fix Pack 1 was successful.
2. Remove the folder *ITM_home*/<*old_platform_code*>/d4_old.
3. Remove the file *ITM_home*/registry/d4<*old_platform_code*>.dep.

Configuring the monitoring agent

Use the following steps to configure the monitoring agent on Linux or UNIX operating systems:

1. Navigate to the *ITM_home*/bin directory, and run the following command:
   ```
   ./itmcmd config -A d4
   ```
   For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
2. Press Enter when you are asked if the monitoring agent connects to a monitoring server.
3. Enter the host name for the monitoring server.
4. Enter the type of protocol that the monitoring agent uses to communicate with the monitoring server. You have four choices
   - ip
   - sna
   - ip.pipe
   - ip.spipe

   Press Enter to accept the default protocol (`ip.pipe`).
5. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use a backup protocol, press Enter without specifying a protocol. If the method that you identified as Protocol 1 fails, Protocol 2 is used. See the *IBM Tivoli Monitoring: Installation and Setup Guide* for more information about available protocol selections.
6. Depending on the types of protocols that you specified, provide the information described in Table 9 on page 94 when prompted:

Table 9. Linux and UNIX Protocol settings for communicating between the monitoring agent and Tivoli Enterprise Monitoring Server

Protocol	Value	Description
IP	IP Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is 1918.
IP.PIPE	IP.PIPE Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is 1918.
IP.SPIPE	IP.SPIPE Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is 3660.
SNA	Network Name	The SNA network identifier for your location.
	LU Name	The LU name for the Tivoli Enterprise Monitoring Server. This LU name corresponds to the local LU Alias in your SNA communications software.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is CANCTDCS.

7. Press Enter to *not* specify the name of the KDC_PARTITION.
8. Press Enter when you are prompted to configure the connection to a secondary monitoring server. The default response is no.
9. Press Enter to accept the default for the Optional Primary Network Name.

Changing the file permissions for agents

If you used a non-root user to install the ITCAM for SOA monitoring agent on a Linux or UNIX operating system, the file permissions are initially set to a low level. Use the following procedure to change these file permissions:

1. Log on to the computer as root, or run the **su** command to become the root user.
2. Create a group (such as itmusers) to own all of the files in the IBM Tivoli Monitoring installation directory. Run one of the following commands:

   For supported Linux, HP-UX, and Solaris operating systems, run the following command:

   ```
   groupadd itmusers
   ```

   For supported AIX operating systems, run the following command:

   ```
   mkgroup itmusers
   ```

3. Change to *ITM_Home* (for information about resolving directory path variables, see "Resolving directory path variables" on page xvi).

   Attention: Running the following steps in the wrong directory can change the permissions for every file in every file system on the computer.
4. Run the following command to ensure that you are in the correct directory:

   ```
   pwd
   ```

5. Run the following commands:

   ```
   chgrp -R itmusers .
   chmod -R g+rwx .
   ```

6. Run the following command to change the ownership of additional agent files:

   ```
   bin/SetPerm
   ```

7. To run the agent as a particular user, add the user to the `itmusers` group. To do this, edit the `/etc/group` file and ensure that the user is in the list of users for the `itmusers` group.

   For example, if you want to run the agent as user `test1`, ensure that the following line is in the`/etc/group` file:

   ```
   itmusers:x:504:test1
   ```
8. Run the **`su`** command to switch to the user that you want to run the agent as or log in as that user.
9. For all monitored environments except for a DataPower environment:
   a. If the application servers that are being monitored were installed as a different user than the one that was used to install and run the ITCAM for SOA monitoring agent, add the user which owns the application server environment to the group created in the previous step. (For information about the access permissions that are needed by the application server user, see the data collector-specific chapters in Part 3 (ITCAM Data Collector for WebSphere) and Part 4 (ITCAM for SOA data collectors).
   b. Navigate to the `*ITM_home*/*platform*/d4/KD4` directory and run the following command:

      ```
      chmod -R g+rwx
      ```

      For information about resolving directory path and platform variables, see "Resolving directory path variables" on page xvi.
   c. Switch to the user for the application server runtime environment.
   d. Enable the data collector by following the procedures that are documented in Part 3 and Part 5 for the specific application server runtime environment.
10. If you are monitoring a DataPower environment, enable the data collector with the same user that runs the monitoring agent. The user can be the same user who installed the agent. For more information about enabling data collection for the DataPower environments, see Chapter 17, "Configuring data collection: DataPower SOA Appliance," on page 441.

During installation, you might see messages displayed similar to these examples:

```
tar: can't set time on gsk7bas64/install: Not owner
tar: can't set time on gsk7bas64/reloc/ibm/gsk_64/bin: Not owner
tar: can't set time on gsk7bas64/reloc/ibm/gsk_64/classes/jre: Not owner
tar: can't set time on gsk7bas64/reloc/ibm/gsk_64/classes/jre/lib: Not owner
tar: can't set time on gsk7bas64/reloc/ibm/gsk_64/classes/jre/lib/ext: Not owner
tar: can't set time on gsk7bas64/reloc/ibm/gsk_64/classes: Not owner
tar: can't set time on gsk7bas64/reloc/ibm/gsk_64/classes/native: Not owner
tar: can't set time on gsk7bas64/reloc/ibm/gsk_64/icc/icclib: Not owner
tar: can't set time on gsk7bas64/reloc/ibm/gsk_64/icc: Not owner
```

These messages do not affect the installation, and can be ignored. You might choose to change the permissions for these files to eliminate these messages.

Silent installation on Linux and UNIX systems

In addition to installing the ITCAM for SOA agent interactively, the installer supports a silent mode. In this mode, no user interaction is required for an installation or uninstallation. Instead, the parameters are taken from a *response* file. You can install and uninstall the ITCAM for SOA agent and install application support files in silent mode.

Response files have a text format. You can create a response file that is based on one of the samples that are provided on the installation DVD or image.

You can also create a response file during installation, modify it if necessary, and then use it for a silent installation. In this way, you can reproduce similar configuration many times, for example, on different hosts.

Installing the ITCAM for SOA Agent with a response file

You can use the installer to install ITCAM for SOA agent in silent mode. To install the agent in silent mode, modify the sample files that are on the installation DVD or image, and then run the installer on the command line.

The `silent_install.txt` sample response file specifies the installation parameters for installing Tivoli Monitoring components and the ITCAM for SOA agent. For more information about using the sample response file to install Tivoli Monitoring components, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

To install ITCAM for SOA in silent mode, complete the following procedure:

1. In the top-level directory of the product installation DVD or image, locate the `silent_install.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify the following property, if necessary. Do not modify any other properties.

Table 10. ITCAM for SOA installation response file properties

Parameter	Definition
EncryptionKey	Required. The data encryption key used to encrypt data that is sent between systems. This key must be the same for all components in your IBM Tivoli Monitoring environment.

4. Save the edited copy in a work directory, for example, as `/tmp/silent.txt`.
5. Run the following command to install ITCAM for SOA in the `/opt/IBM/ITM` directory:

```
./install.sh -q -h install_dir -p response_file
```

Where:

install_dir
Identifies the installation location for the IBM Tivoli Monitoring component. The default installation location is `/opt/IBM/ITM`.

response_file
Identifies the response file that you edited to specify the installation parameters. Specify the absolute path to this file.

For example:

```
./install.sh -q -h /opt/ibm/itm -p /tmp/silent_install.txt
```

The sample `silent_install.txt` file presents all of the parameters that are required for installing Tivoli Monitoring. The file contains comments that explain each of the options.

Performing a silent uninstallation

To uninstall the ITCAM for SOA agent in silent mode:

1. Change to the *ITM_home*/bin directory.
2. Run the following command:

   ```
   ./uninstall.sh -f d4 platform_code
   ```

   Where:

   -f Forces delete, suppressing confirmation messages and prompts.

   d4 Is the 2-letter code for the product to be uninstalled.

   Platform
   Is the platform code for the product. To determine the platform code for your platform, see "Determining the *platform* value in directory paths" on page xvii

Remember: If the ITCAM Data Collector for WebSphere home directory was specified to be outside of the IBM Tivoli Monitoring home directory, the ITCAM Data Collector for WebSphere home directory is not removed during the uninstallation.

For more information about installing Tivoli Monitoring in silent mode, see "Appendix B. Performing a silent installation of IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Configuring for remote deployment of the monitoring agent

ITCAM for SOA supports the Tivoli Monitoring feature of remotely deploying the monitoring agent across your environment from a central location, the monitoring server.

Before you install the ITCAM for SOA on a remote system using Tivoli Enterprise Portal, the application support files must be installed on the Tivoli Enterprise Portal Server (including browser client support files), hub and remote Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal desktop clients.

Installation of application support files is only required when the monitoring agent is deployed from the Tivoli Enterprise Portal. However, the application support files must be installed to view monitoring data in the Tivoli Enterprise Portal, regardless of whether the agent was installed remotely with the Tivoli Enterprise Portal or from the command-line interface.

The application support files are automatically propagated to the monitoring server, if all of the following conditions are met:

- Self-description is enabled on the hub and remote monitoring servers
- All Tivoli Management Services server components are at version 6.2.3 or higher.
- The agent framework is at version 6.2.3 or higher.

Self-description is enabled by default on ITCAM for SOA. For more information about the conditions that must be met for self-description, see "Enabling application support through self-description" on page 36.

For more information about remote deployment in an IBM Tivoli Monitoring environment, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Adding the installation bundles to the deployment depot

Before you can deploy the monitoring agent to a remote computer, you must add the operating-system-specific monitoring agent bundle to the deployment depot. For example, if you are deploying the monitoring agent to a Linux operating system, the bundle for Linux must be added to the deployment depot.

If you installed application support files for the monitoring server, you might have already added the monitoring agent to the deployment depot during the installation. If not, you can add the monitoring agent bundle to the deployment depot at any time with the following method:

1. Copy or mount the ITCAM for SOA monitoring agent installation images on the monitoring server host.
2. Change to the *ITM_HOME*/bin directory.

   For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
3. Run the following command to log in to the monitoring server:

   ```
   ./tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the Tivoli Monitoring SYSADMIN user and the password for the SYSADMIN user.

   For example:

   ```
   ./tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
4. (Optional) List the available bundles for the specific operating system in the *path_to_Linux_UNIX_image*/unix/deploy directory with the following command:

   ```
   ./tacmd listBundles -i path_to_Linux_UNIX_image/unix/deploy
   ```
5. To add the installation bundle for Linux or UNIX target hosts, enter this command:

   ```
   ./tacmd addBundles -i path_to_Linux_UNIX_image/unix -t d4
   ```

   The code d4 is the product code for the ITCAM for SOA monitoring agent.

For more information about this procedure, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing the monitoring agent remotely with Tivoli Enterprise Portal

You can use the Tivoli Enterprise Portal to install the monitoring agent remotely.

Before you install the ITCAM for SOA monitoring agent on a remote system, the application support files must be installed on the Tivoli Enterprise Portal Server (including the browser client support files), hub and remote Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal desktop clients.

Before you can install the ITCAM for SOA monitoring agent on a remote system, you must first deploy an OS monitoring agent to the remote system. See the *IBM Tivoli Monitoring: Installation and Setup Guide* for details.

To install the monitoring agent remotely with Tivoli Monitoring, complete the following procedure:

1. From the physical Navigator view in the Tivoli Enterprise Portal, navigate to the computer where you want to install the monitoring agent.
2. Right-click the remote computer and select **Add Managed System**.

3. Select **Monitoring Agent for Composite Application Manager for SOA** from the list of available bundles and click **OK**.
4. The New Managed System Configuration window is displayed. Accept the default to use the local system account or specify a valid account and password.
5. Click **Finish**. The monitoring agent installation process is started; you can track its progress in the **Deployment Status** workspace.

This procedure installs the monitoring agent and the ITCAM for SOA-specific data collectors.

Restriction: The procedure does not install the Data Collector for WebSphere Message Broker. To install the Data Collector for WebSphere Message Broker on a remote system, copy the ITCAM for SOA installation media to the remote system, run the installation program, and choose the Data Collector for WebSphere Message Broker from the list of features that are available for installation.

To install and configure the ITCAM Data Collector for WebSphere, see "Installing and configuring ITCAM Data Collector for WebSphere from a command line" on page 100.

For more information about this procedure, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing the monitoring agent remotely from a command line

You can install the monitoring agent to a remote system with the command prompt on the monitoring server.

You do not have to install application support files on the Tivoli Enterprise Portal Server, hub and remote Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal desktop clients before you install the agent remotely from the command prompt. However, the application support files must be installed to view monitoring data in the Tivoli Enterprise Portal after remote deployment.

Before you can install the ITCAM for SOA monitoring agent on a remote system, you must first deploy an OS monitoring agent to the remote system. See the *Tivoli Monitoring: Installation and Setup Guide* for details.

For details on using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

To install the monitoring agent on the command line, complete the following procedure on the monitoring server:

1. Change to the `*ITM_HOME*/bin` directory.

   For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
2. Use the following command to log in to the monitoring server:

   ```
   ./tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user of Tivoli Monitoring and password. For example:

   ```
   ./tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
3. To install the ITCAM for SOA monitoring agent on a remote host, enter the **`tacmd addSystem`** command, specifying `d4` as the product code for the ITCAM for SOA monitoring agent:

```
./tacmd addSystem -t d4 -n Primary:SOAWIN48:NT
```

4. To monitor the remote deployment status, enter the following command:

   ```
   ./tacmd getDeployStatus
   ```

For more information about this procedure, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

This procedure installs the monitoring agent and the ITCAM for SOA-specific data collectors.

Restriction: The procedure does not install the Data Collector for WebSphere Message Broker. To install the Data Collector for WebSphere Message Broker on a remote system, copy the ITCAM for SOA installation media to the remote system, run the installation program, and choose the Data Collector for WebSphere Message Broker from the list of features that are available for installation.

To install and configure the ITCAM Data Collector for WebSphere, see "Installing and configuring ITCAM Data Collector for WebSphere from a command line."

When the monitoring agent is successfully installed, it connects automatically to the monitoring server, and the portal desktop shows the monitoring agent.

Installing and configuring ITCAM Data Collector for WebSphere from a command line

You can install and configure ITCAM Data Collector for WebSphere using `tacmd` commands on a remote system from the command prompt of the monitoring server.

You must install the monitoring agent on the remote system from the monitoring server before you install ITCAM Data Collector for WebSphere.

When you install monitoring agent on the remote system, ITCAM Data Collector for WebSphere installation files are placed in the *ITM_Home*/*arch*/KD4/wasdc directory. The directory contains the following files:

- Data collector installation files, `itcam_gdc.tar.gz`.
- A script to extract and install the installation files, `gdc_extract.sh`.

For more information about operating system-dependent variables, see "Determining the *platform* value in directory paths" on page xvii.

Tip: In the following procedure, if the monitoring server is on a Windows system, use the `tacmd` command. If the monitoring server is on a Linux or UNIX system, use the `./tacmd` command.

You can use `tacmd executecommand` to install the data collector and configure it in silent mode. To use the `tacmd executecommand` command, the hub and remote monitoring servers must be at version 6.2.2 fix pack 2 or later. For details about using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

To install the ITCAM Data Collector for WebSphere from the command line, complete the following procedure from the monitoring server:

1. Change to *ITM_HOME*/bin directory.
2. Use the following command to log in to the monitoring server:

```
./tacmd login -s TEMS_hostname -u userid -p password
```

Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

```
./tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
```

3. Set the `KT1_TEMS_SECURE` configuration parameter in the hub monitoring server's configuration file to specify that the hub monitoring server supports the `tacmd` commands:
   - Navigate to the file *ITM_Home*`/config/ms.ini`.
   - Set the property to `KT1_TEMS_SECURE='YES'`.
   - Recycle the monitoring server.
4. Set the location of the Java home directory, the Tivoli Monitoring home directory, and the data collector home directory. Extract the data collector installation files to the data collector home directory.

```
 ./tacmd  executecommand -m System -c "export JAVA_HOME=path_to_java_home&&export CANDLE_HOME=path_to_ITM_home&&
./gdc_extract.sh -d path_to_dc_home full_path_to_archive_file"
-w ITM_Home/arch/KD4/wasdc
```

Where:

-m|--system
: Specifies on which OS agent to run the command. Run the **`tacmd listSystems`** command to list the OS agents that you are monitoring. For example:

```
./tacmd listSystems -t UX LZ NT
```

-c|--commandstring
: Specifies the command to run. Use double quotation marks for commands with parameters. You must escape back slashes when defining a Windows directory path. For more information, see the "Escaping backslashes, spaces, and double quotation marks" section in the *Tivoli Monitoring Command Reference* guide.

-w|--workingdir
: Specifies the working directory that is switched to before the command is run. When running this command between a UNIX or Linux system and targeting a Windows monitoring agent, you must replace the backslashes with forward slashes in the path definitions for the source parameter. It is best to use forward slashes for tolerance with Windows systems. If the working directory contains spaces, you must include double quotation marks around the directory location

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "export JAVA_HOME=/opt/IBM/ITM/JRE/li6263&&export
CANDLE_HOME=/opt/IBM/ITM&&./gdc_extract.sh -d /opt/IBM/ITM/dchome1 /opt/IBM/ITM/li6263/KD4/wasdc/
itcam_gdc.tar.gz"
-w /opt/IBM/ITM/li6263/KD4/wasdc
```

On Solaris systems:

```
 ./tacmd  executecommand -m v5254005b0186:KUX -c "JAVA_HOME=/opt/IBM/ITM/JRE/sol283&&export JAVA_HOME&&
./gdc_extract.sh -d /opt/IBM/ITM/dchome1 /opt/IBM/ITM/sol283/KD4/wasdc/itcam_gdc.tar.gz"
-w /opt/IBM/ITM/sol283/KD4/wasdc
```

5. Specify the data collector configuration in a properties file on the monitoring server. A sample properties file, `sample_silent_config.txt`, is available from *DC_home*`/bin` on any local system where you installed the agent.
6. Copy the *silent_file* from the monitoring server to the remote system using the `tacmd putfile` command.

```
./tacmd putfile -m System -s local_dir_path/silent_file -d remote_dir_path/silent_file -t text
```

Where:

-m|--system
: Specifies on which OS agent to run the command. Run the **tacmd listSystems** command to list the OS agents that you are monitoring. For example:

```
./tacmd listSystems -t UX LZ NT
```

-s|--source
: Specifies the local file name.

-d|--destination
: Specifies the remote file name.

-t|--text
: Specifies the mode of transfer.

For example:

```
./tacmd putfile -m v5254005b0186:LZ -s dc_config.txt -d /opt/IBM/ITM/dchome1/7.2.0.0.4/bin/dc_config.txt -t text
```

7. Configure the data collector using the silent response file:

```
./tacmd executecommand -m System -c "./config.sh -silent /full_path_to_silent_file/silent_file.txt"
-w path_to_DC_home/bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./config.sh -silent /opt/IBM/ITM/dchome1/7.2.0.0.4/bin/dc_config.txt"
-w /opt/IBM/ITM/dchome1/7.2.0.0.4/bin
```

8. Restart the application server instances.
   a. Stop the application server.

```
./tacmd executecommand -m System -c "./stopServer.sh server_name" -w profile_home/bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./stopServer.sh server3" -w /opt/IBM/WAS8/profiles/AppSrv01/bin
```

   b. Start the application server:

```
./tacmd executecommand -m System -c "./startServer.sh server_name" -w profile_home\bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./startServer.sh server3" -w /opt/IBM/WAS8/profiles/AppSrv01/bin
```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Upgrading a remotely deployed monitoring agent

To upgrade or update an existing remotely deployed ITCAM for SOA monitoring agent on a specified managed system to a newer version, add the new version of the monitoring agent to the deployment depot and then use the **tacmd updateAgent** command to upgrade the monitoring agent. This command is documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Remember: ITCAM for SOA supports only a single installation per computer system.

You might already have a previous version (version 7.1.1 or version 7.2) of the ITCAM for SOA monitoring agent deployed to a remote system in your environment. With the remote agent deployment function of Tivoli Monitoring, you can populate the deployment depot with newer versions of your monitoring agent and use the remote deployment function to upgrade or update to the newer version.

Before you can remotely deploy a newer version of the monitoring agent, you must first deploy an OS agent to the remote system. Deploy this OS agent to the same Tivoli Monitoring installation directory (*ITM_home*) as the installation directory of the existing version of the ITCAM for SOA monitoring agent. When you deploy the new version of the monitoring agent, you must also specify the same directory where the OS agent is installed. This ensures that the previous version of the monitoring agent is upgraded.

This procedure upgrades the monitoring agent and the ITCAM for SOA-specific data collectors.

To migrate the ITCAM Data Collector for WebSphere, see "Migrating to the ITCAM Data Collector for WebSphere from a command-line."

To migrate the WebSphere Message Broker data collector, you must copy the agent installation media to the remote system, and follow the upgrade procedure in "Upgrading to the Data Collector for WebSphere Message Broker" on page 360.

Migrating to the ITCAM Data Collector for WebSphere from a command-line

When you upgrade to ITCAM for SOA version 7.2 or later on the remote system, there may be other older versions of the data collector installed and configured for the same profile in which you plan to configure ITCAM for SOA.

These older versions of the data collector must be migrated to the ITCAM Data Collector for WebSphere after you install ITCAM Data Collector for WebSphere. The ITCAM for SOA 7.1.1 data collector for the WebSphere Application Server is upgraded automatically as part of the migration of these older versions of the data collector.

When an earlier maintenance level of the ITCAM Data Collector for WebSphere is installed and configured for the same profile, you can migrate it to the latest maintenance level using the ITCAM Data Collector for WebSphere Migration utility.

You can use `tacmd executecommand` to migrate older versions and earlier maintenance levels of the data collector in silent mode. For details about using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

In the following procedure, if the monitoring server is on a Windows system, use the `tacmd` command. If the monitoring server is on a Linux or UNIX system, use the `./tacmd` command.

Remember: You must upgrade the monitoring agent on the remote system before you upgrade the data collector.

To migrate an older version or an earlier maintenance level of the data collector to the latest ITCAM Data Collector for WebSphere with the command prompt, complete the following procedure on the monitoring server:

1. Change to *`ITM_HOME`*`/bin` directory.
2. Use the following command to log in to the monitoring server:

```
./tacmd  login -s TEMS_hostname -u userid -p password
```

Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

```
./tacmd  login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
```

3. Set the KT1_TEMS_SECURE configuration parameter in the hub monitoring server's configuration file to specify that the hub monitoring server supports the tacmd commands:
   - Navigate to the file *ITM_Home*/config/ms.ini.
   - Set the property to KT1_TEMS_SECURE='YES'.
   - Recycle the monitoring server.
4. Set the location of the Java home directory, the Tivoli Monitoring home directory, and the data collector home directory. Extract the data collector installation files to the data collector home directory.

```
 ./tacmd  executecommand -m System -c "export JAVA_HOME=path_to_java_home&&export CANDLE_HOME=path_to_ITM_home&&
./gdc_extract.sh -d path_to_dc_home full_path_to_archive_file"
-w ITM_Home/arch/KD4/wasdc
```

Where:

-m|--system
Specifies on which OS agent to run the command. Run the **tacmd listSystems** command to list the OS agents that you are monitoring. For example:

```
./tacmd listSystems -t UX LZ NT
```

-c|--commandstring
Specifies the command to run. Use double quotation marks for commands with parameters. You must escape back slashes when defining a Windows directory path. For more information, see the "Escaping backslashes, spaces, and double quotation marks" section in the *Tivoli Monitoring Command Reference* guide.

-w|--workingdir
Specifies the working directory that is switched to before the command is run. When running this command between a UNIX or Linux system and targeting a Windows monitoring agent, you must replace the backslashes with forward slashes in the path definitions for the source parameter. It is best to use forward slashes for tolerance with Windows systems. If the working directory contains spaces, you must include double quotation marks around the directory location

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "export JAVA_HOME=/opt/IBM/ITM/JRE/li6263&&export
CANDLE_HOME=/opt/IBM/ITM&&./gdc_extract.sh -d /opt/IBM/ITM/dchome1 /opt/IBM/ITM/li6263/KD4/wasdc/
itcam_gdc.tar.gz"
-w /opt/IBM/ITM/li6263/KD4/wasdc
```

On Solaris systems:

```
 ./tacmd  executecommand -m v5254005b0186:KUX -c "JAVA_HOME=/opt/IBM/ITM/JRE/sol283&&export JAVA_HOME&&
./gdc_extract.sh -d /opt/IBM/ITM/dchome1 /opt/IBM/ITM/sol283/KD4/wasdc/itcam_gdc.tar.gz"
-w /opt/IBM/ITM/sol283/KD4/wasdc
```

5. Specify the migration details in a properties file on the monitoring server. Two sample properties file are available from *DC_home*/bin on any local system where you installed the agent.

   The file, sample_silent_migrate.txt, can be used when you migrate the data collector of the following products to the ITCAM Data Collector for WebSphere:
   - ITCAM for WebSphere 6.1.0.4 or later

- WebSphere Data Collector 6.1.0.4 or later included in ITCAM for Web Resources 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications 7.1 included in ITCAM for Applications Diagnostics 7.1
- ITCAM for WebSphere Application Server 7.2

The file, `sample_silent_migrate_soa.txt`, can be used when you migrate the ITCAM for SOA 7.1.1 data collector to the ITCAM Data Collector for WebSphere.

6. Copy the *silent_file* from the monitoring server to the remote system using the `tacmd putfile` command.

```
./tacmd putfile -m System -s local_dir_path/silent_file -d remote_dir_path/silent_file -t text
```

Where:

-m|--system
Specifies on which OS agent to run the command. Run the **`tacmd listSystems`** command to list the OS agents that you are monitoring. For example:

```
./tacmd listSystems -t UX LZ NT
```

-s|--source
Specifies the local file name.

-d|--destination
Specifies the remote file name.

-t|--text
Specifies the mode of transfer.

For example:

```
./tacmd putfile -m v5254005b0186:LZ -s dc_config.txt -d /opt/IBM/ITM/dchome1/7.2.0.0.4/bin/dc_config.txt -t text
```

7. Configure the data collector using the silent response file:

```
./tacmd executecommand -m System -c "./migrate.sh -silent /full_path_to_silent_file/silent_file.txt"
-w path_to_DC_home/bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./migrate.sh -silent /opt/IBM/ITM/dchome1/7.2.0.0.4/bin/dc_config.txt"
-w /opt/IBM/ITM/dchome1/7.2.0.0.4/bin
```

8. Restart the application server instances.
   a. Stop the application server.

```
./tacmd executecommand -m System -c "./stopServer.sh server_name" -w profile_home/bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./stopServer.sh server3" -w /opt/IBM/WAS8/profiles/AppSrv01/bin
```

   b. Start the application server:

```
./tacmd executecommand -m System -c "./startServer.sh server_name" -w profile_home\bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./startServer.sh server3" -w /opt/IBM/WAS8/profiles/AppSrv01/bin
```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Enabling the ITCAM for SOA data collectors on the remote system

After you install the monitoring agent remotely on one or more managed systems, you must enable the ITCAM for SOA data collectors for the application server runtime environments that are being monitored on each remote system. To enable the data collectors, run the Data Collector Configuration utility or run the `KD4configDC` script as described in Part 4, "Configuring ITCAM for SOA-specific data collectors for runtime environments," on page 373.

The ITCAM for SOA data collector can be installed and configured remotely using the procedures in Part 4, "Configuring ITCAM for SOA-specific data collectors for runtime environments," on page 373.

Uninstalling IBM Tivoli Composite Application Manager for SOA on Linux or UNIX systems

After you upgrade your Tivoli Monitoring environment, you cannot restore the environment to the previous level. If you uninstall Tivoli Monitoring after an upgrade, all of Tivoli Monitoring is removed, and any subsequent installation is equivalent to installing for the first time.

The same is true for ITCAM for SOA. After you upgrade your environment from a previous version of ITCAM for SOA to version 7.2 or later, there is no way to return to the previous version. If you uninstall ITCAM for SOA after an upgrade, all of ITCAM for SOA is removed, and any subsequent installation is equivalent to installing for the first time.

Tivoli Monitoring does not support uninstalling the ITCAM for SOA application support files from the Tivoli Monitoring environment. After you install the ITCAM for SOA application support files on a Tivoli Enterprise Portal, Tivoli Enterprise Portal Server or Tivoli Enterprise Monitoring Server computer, there is no way to remove these support files without completely uninstalling all of Tivoli Monitoring.

This also means that you cannot uninstall the SOA Domain Management Server or Tivoli Common Object Repository support from the Tivoli Enterprise Portal Server configuration, or remove it from the Tivoli Enterprise Portal Server computer.

To uninstall IBM Tivoli Composite Application Manager for SOA from your services environment, complete the tasks in the next sections.

Before uninstalling the monitoring agent

Before you install the monitoring agent, complete the following tasks:

1. If the system is running a Tivoli Enterprise Portal desktop or browser client, close it.
2. Open Manage Tivoli Enterprise Monitoring Services. If any of the following services are running, stop them. Right-clicking the services and selecting **Stop** from the menu):
   - The ITCAM for SOA monitoring agent
   - Tivoli Enterprise Portal Server
   - Tivoli Enterprise Monitoring Server
3. Close the Manage Tivoli Enterprise Monitoring Services utility.

4. If you have not done so, disable data collection for your runtime environments. Follow the procedures in Part 4, "Configuring ITCAM for SOA-specific data collectors for runtime environments," on page 373. You might have to stop affected application servers as part of the procedure.

   Beginning with ITCAM for SOA version 7.2, you no longer disable data collection for the ITCAM Data Collector for WebSphere by using the ITCAM for SOA `ConfigDC` utility. Instead, use the ITCAM Data Collector for WebSphere Unconfiguration utility to disable data collection. For more information about unconfiguring the ITCAM Data Collector for WebSphere, see "Unconfiguring ITCAM Data Collector for WebSphere" on page 282.

   Restriction: If you are running BEA WebLogic Server application server environments, you do not have to stop this service now to perform the agent uninstallation. However, after you uninstall the agent, stop and restart the application server at a later time (for example, during off-shift hours).

Considerations for uninstalling WebSphere Application Server data collector

If you are uninstalling the monitoring agent because you want to reinstall the ITCAM for SOA WebSphere Application Server data collector and reconfigure data collection for a WebSphere Application Server, you must not delete `KD4.dc.properties` properties file or the *`ITCAM4SOA_Home`*`\KD4` directory after uninstalling the data collector. Instead, navigate to the `/KD4/config` directory and manually remove the following properties from the `KD4.dc.properties` file before you uninstall the monitoring agent:

- `kd4.ira.supportsFile.service`
- `kd4.ira.supportsFile.staticBPM`
- `Kd4.ira.supportsFile.dynamicBPM`
- `kd4.ira.supportsFile.dynamicBPD`

Uninstalling the monitoring agent on Linux or UNIX systems

Uninstall the monitoring agent on supported Linux, AIX, HP-UX, and Solaris operating systems by navigating to *`ITM_Home`*`/bin` folder and running the **`./uninstall.sh`** command. (For information about resolving directory path variables, see "Resolving directory path variables" on page xvi). Follow the on-screen prompts to complete the uninstallation.

Important: If the home directory of ITCAM Data Collector for WebSphere is outside of the IBM Tivoli Monitoring home directory, the data collector home directory is not removed during the uninstallation and must be removed manually.

Removing tables from the warehouse database

If you configured historical data collection, you might still have a database installed. The database is not deleted as part of this uninstall process, because other IBM Tivoli monitoring agents might also be using it. Follow the procedures in your database software publications for removing any unwanted tables from the warehouse database.

Removing files and folders

When you uninstall ITCAM for SOA, navigate to the *`ITCAM4SOA_Home`*`/KD4/config` folder and either clear or delete the `KD4.dc.properties` file. If you do not clear or delete this properties file, and later install the monitoring agent again, the configuration settings for data collector control remain at the settings that were used for the previous installation and not the default settings.

You must delete the `ITCAM4SOA_Home/KD4` folder, where *ITCAM4SOA_Home* is the directory location where the ITCAM for SOA monitoring agent is installed. See "The IBM Tivoli Composite Application Manager for SOA home directory" on page xvi for information about how to determine the value of *ITCAM4SOA_Home*.

Important: When you uninstall ITCAM for SOA because you want to reinstall the ITCAM for SOA version 7.1.1 data collector and reconfigure data collection for the WebSphere Application Server, do no clear or delete the `KD4.dc.properties` file or delete the `ITCAM4SOA_Home/KD4` folder. Instead, delete the properties that are specified in "Considerations for uninstalling WebSphere Application Server data collector" on page 107 from the `KD4.dc.properties` file.

Removing SOA Domain Management Server and Tivoli Common Object Repository databases

The database that is used with SOA Domain Management Server and Tivoli Common Object Repository are not deleted as part of the uninstallation process. Follow the procedures in your database application software publications for removing an unused database.

Installing and uninstalling language support

A Language Pack enables user interaction with the monitoring agent in a language other than English. For example, when a Spanish language pack is installed, the Tivoli Enterprise Portal Server workspaces and the internal messages of the monitoring agent are displayed in Spanish.

To enable full support for a language, you must install the language pack on the monitoring agent host and all hosts where the monitoring agent support files are installed (Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and all Tivoli Enterprise Portal desktop clients).

If you no longer want to use a language, uninstall the language pack for the language.

Remember: This procedure assumes that language support for the same language is installed on Tivoli Monitoring. If not, see the *IBM Tivoli Monitoring: Installation and Setup Guide* and install the base language support for Tivoli Monitoring before installing language support for the monitoring agent.

Installing a language pack on UNIX or Linux systems

To install a language pack, first make sure that you already installed the product in English, then complete the following steps:

1. Run the following command to create a temporary directory on the computer. Make sure that the full path of the directory does not contain any spaces:
   ```
   mkdir dir_name
   ```
2. Mount the language pack installation image to the temporary directory that you just created.
3. Run the following commands to start the installation program:
   ```
   cd dir_name
   lpinstaller.sh -c ITM_home
   ```

For information about resolving directory path variables, see “Resolving directory path variables” on page xvi

Tip: *ITM_home* is the location where you installed IBM Tivoli Monitoring. For Linux and UNIX operating systems, it is typically `/opt/IBM/ITM`.

4. Select the language of the installer and click **OK**.

   Important: In this step, you select the language for the installer user interface, not the language pack that is to be installed.
5. Click **Next** on the Introduction panel.
6. Click **Add/Update** and click **Next**.
7. Select the directory where the National Language Support package (NLSPKG) files are located. This is the `nlspackage` directory on the language pack installation image.
8. Select the agent for which you want to process national language support and click **Next**.
9. Select the languages to install and click **Next**.

   Tip: You can hold down the **Ctrl** key for multiple selections.
10. Examine the installation summary page and click **Next** to begin the installation.
11. Click **Done** after the installation completes to exit the installer.
12. Start the Manage Tivoli Enterprise Monitoring Services utility and restart Tivoli Enterprise Portal Desktop Client and Tivoli Enterprise Portal Server. If the Help Server is running, restart it also.

Uninstalling a language pack on UNIX or Linux

To uninstall a language pack, complete the following steps:

1. Mount the language pack installation image.
2. Run the following commands to start the installation program:

   ```
   cd dir_name
   lpinstaller.sh -c ITM_home
   ```

   ITM_home is the location where you installed IBM Tivoli Monitoring. For Linux and UNIX operating systems, it is typically `/opt/IBM/ITM`.
3. Select the language of the installer and click **OK**.

   Important: In this step, you select the language for the installer user interface, not the language pack that is to be uninstalled.
4. Click **Next** on the Introduction panel.
5. Select **Remove** and click **Next**.
6. Select the agent for which you wish to remove national language support and click **Next**.
7. Select the languages to uninstall and click **Next**.

   Tip: You can hold down the **Ctrl** key for multiple selections.
8. Examine the uninstallation summary page and click **Next** to begin the uninstallation process.
9. Click **Done** to exit the installer.

10. Start the Manage Tivoli Enterprise Monitoring Services utility and restart Tivoli Enterprise Portal Desktop Client and Tivoli Enterprise Portal Server. If the Eclipse Help Server is running, restart it as well.

Chapter 4. Configuring topology support on Windows systems

Topology support provides views of service-to-service relationships and the relationship between services and service registry information and business process information.

Overview

ITCAM for SOA supports the discovery, storage, and display of information about service resources (application servers, service ports, and operations) and the relationships between them. These service-to-service relationships and flows can then be displayed in Tivoli Enterprise Portal topology workspaces and views.

ITCAM for SOA provides two key components for this topology support:

SOA Domain Management Server
Stores information about service resources and service-to-service relationships and flows. It can retrieve service registry and business process integration information from the Tivoli Common Object Repository, if present, to display this information in topology workspaces and views.

Tivoli Common Object Repository
Stores service registry and business processes integration topology data that is retrieved from one or more discovery library adapters.

Installing and configuring topology support

To install and configure topology support for ITCAM for SOA version 7.2 fix pack 1, complete the following steps:

1. Create the SOA Domain Management Server database on the Tivoli Enterprise Portal Server (or remotely on a different server).

   Use the database creation scripts that come with ITCAM for SOA and start the database. If you are using a DB2 or Microsoft SQL Server database, you can create the database locally with the SOA Domain Management Server Configuration utility. If you are using an Oracle database, you must create the database manually.
2. (Optional) Create the Tivoli Common Object Repository database on the Tivoli Enterprise Portal Server (or remotely on a different server).

   Use the database creation scripts that come with ITCAM for SOA and start the database. If you are using a DB2 database, you can create the database with the SOA Domain Management Server Configuration utility. If you are using an Oracle database, you must create the database manually.
3. Run the SOA Domain Management Server Configuration utility.

   If you created the databases already, select the option to use an existing database and complete the configuration of the database.

   If you did not create the databases already, select the option to create each database locally and complete the configuration of the database.
4. Reconfigure and restart the Tivoli Enterprise Portal Server.

Upgrading or updating topology support

To upgrade topology support to ITCAM for SOA version 7.2 or update topology support to ITCAM for SOA version 7.2 fix pack 1, complete the following steps:

1. Verify that the SOA Domain Management Server database and the Tivoli Common Object Repository database (if installed) are started.
2. If the SOA Domain Management Server or the Tivoli Common Object Repository are on a remote server, run the migration scripts that are provided by ITCAM for SOA.
3. Run the SOA Domain Management Server Configuration utility to perform the upgrade.
   If the databases are located remotely, run the utility with the `-remoteSDMS` or the `-remoteTCORE` arguments.
4. Reconfigure and restart the Tivoli Enterprise Portal Server.

Detailed instructions on how to perform each of the upgrade steps are provided in the following sections.

Important: If you are upgrading from ITCAM for SOA version 7.1.1, you must upgrade topology support to ITCAM for SOA version 7.2 before you update topology support to version 7.2 fix pack 1.

Topology Views and Configuration Options

When you are planning your installation, consider the following points:

- Whether to install the SOA Domain Management Server and Tivoli Common Object Repository components.
- Whether to use an existing or new database for each component.
- Whether the databases will reside on a remote server or locally on the portal server.
- What type of database to use.

Topology Views

The topology components that you have to install and configure depend on the topology views you want to display:

Table 11. Topology Views

Service-to-Service Topology Views	Service Registry and Business Process Integration Topology Views	Components Required
Yes	No	SOA Domain Management Server
Yes	Yes	SOA Domain Management Server and Tivoli Common Object Repository
No	Yes	SOA Domain Management Server and Tivoli Common Object Repository

Restriction: To display service-to-service topology views or service registry and business progress integration topology views, or both, when you integrate ITCAM for SOA version 7.2 or later with Tivoli Monitoring version 6.2.2, you must install SOA Domain Management Server and Tivoli Common Object Repository.

If you decide to configure only SOA Domain Management Server, create a database for SOA Domain Management Server that is not used by other applications.

If you decide to configure the SOA Domain Management Server and the Tivoli Common Object Repository, the following configuration options are available:

1. Use an existing database that is used by other applications for SOA Domain Management Server and Tivoli Common Object Repository.
2. Create a database for SOA Domain Management Server, and create a separate new database for Tivoli Common Object Repository.
3. Create a database that is shared by both SOA Domain Management Server and Tivoli Common Object Repository. This option is only available when you create the database manually.

Both the SOA Domain Management Server component and the Tivoli Common Object Repository component use either a local or remote database to contain their service resource and topology data. You have the option of configuring the SOA Domain Management Server to operate with or without Tivoli Common Object Repository.

SOA Domain Management Server Configuration Options

If you use an existing database for SOA Domain Management Server and, optionally, for Tivoli Common Object Repository you must run the SOA Domain Management Server Configuration Utility to configure topology support on both components.

If you create an SOA Domain Management Server database manually on the local portal server or on a remote database server, the configuration options that are listed in the following table are available.

Table 12. Options for manually configuring the database server for SOA Domain Management Server

Location	Database Type	Topic
Local	DB2	“Manually creating a DB2 database locally on Windows systems for SOA Domain Management Server” on page 121
Local	Microsoft SQL	“Manually creating a Microsoft SQL Server database locally on Windows systems for SOA Domain Management Server” on page 122
Local	Oracle	“Manually creating an Oracle database locally on Windows systems for SOA Domain Management Server” on page 123
Remote	DB2	“Manually creating a DB2 database remotely on Windows systems for SOA Domain Management Server” on page 124
Remote	Microsoft SQL	“Manually creating a Microsoft SQL Server database remotely on Windows systems for SOA Domain Management Server” on page 125
Remote	Oracle	“Manually creating an Oracle database remotely on Windows systems for SOA Domain Management Server” on page 126

Tip: If this server is installed on the same computer as the portal server, the database server is usually the same database server that is used by the portal server.

Tivoli Common Object Repository Configuration Options

If you manually create a new Tivoli Common Object Repository database, the configuration options listed in the following table are available:

Table 13. Options for manually configuring the database server for Tivoli Common Object Repository

Location	Database Type	Topic
Local	DB2	"Manually creating a DB2 database locally on Windows systems for Tivoli Common Object Repository" on page 128
Local	Oracle	"Manually creating an Oracle database locally on Windows systems for Tivoli Common Object Repository" on page 129
Remote	DB2	"Manually creating a DB2 database remotely on Windows systems for Tivoli Common Object Repository" on page 130
Remote	Oracle	"Manually creating an Oracle database remotely on Windows systems for Tivoli Common Object Repository" on page 131

Important: You require database administrative authority to create the databases that are used with SOA Domain Management Server and Tivoli Common Object Repository. For more information about database permissions, see "Database and User Permissions" on page 115.

Planning topology support on Windows system

Before you configure SOA Domain Management Server and the optional Tivoli Common Object Repository, you must have enough available space on the partition where Tivoli Monitoring is installed. You must know the permissions that are required for creating and configuring the SOA Domain Management Server and Tivoli Common Object Repository databases and the permissions required for the user that is specified as the database administrator.

Minimum space requirements on the file system

Before you configure SOA Domain Management Server and optional Tivoli Common Object Repository, you must have enough available space on the partition where Tivoli Monitoring is installed. When you configure SOA Domain Management Server and optional Tivoli Common Object Repository, you must accommodate the files that are needed for these components, including room for growth for Tivoli Common Object Repository bulk load results files.

For more information about the required hardware for ITCAM for SOA, see "Required hardware" on page 16.

Database and User Permissions

When you run the SOA Domain Management Server Configuration Utility (referred to by its script name, `ConfigDMS`), you must have certain minimum user permissions, depending on the task that you are doing.

Permissions required when installing SOA Domain Management Server or Tivoli Common Object Repository

You require the following permissions when you configure the SOA Domain Management Server and Tivoli Common Object Repository database as part of installing ITCAM for SOA.

DB2 database configuration permissions

The permissions that are required when configuring a DB2 database for SOA Domain Management Server and Tivoli Common Object Repository as part of an installation of ITCAM for SOA are in Table 14:

Table 14. Permissions required when configuring a DB2 database

Task	User and Database Requirements

Permissions required to run the scripts to manually create a DB2 database either locally or remotely	The requirements are as follows:
	• The user must have Windows administrator privileges (for example, exist in Administrators group).
	• The user must have DB2 administrator privileges (for example, exist in DB2ADMNS group).
	• The user must be either a local user or a domain user who has been granted sufficient permissions to create a DB2 database.
	To check whether a user is a local user or a domain user, run the command **`echo %USERDOMAIN%`** from a command prompt. For a local user, the command output displays the host name of the local computer. For a domain user, the command output displays the name of a domain on the network.
	A domain user belongs to a networked domain and does not have sufficient permissions to create a DB2 database. To provide a domain user with sufficient permissions to create a DB2 database, run the following command from a DB2 command window:
	`DB2SET DB2_GRP_LOOKUP=LOCAL,TOKENLOCAL`
	`DB2STOP`
	`DB2START`

Permissions required to run the `ConfigDMS` utility to either (a) configure a DB2 database that was configured locally or remotely, or (b) create the DB2 database locally and configure it	The requirements are as follows: • The user must have Windows administrator privileges (for example, in Administrators group). • The user must have DB2 administrator privileges (for example, in DB2ADMNS group). **Tip:** Not applicable if the database was previously created. • The user must be the user who installed IBM Tivoli Monitoring. • The user must have read, write, and modify permissions for the following directories: – *ITM_HOME*`\CNPS` directory and its subdirectories – *ITM_HOME*`\CNPSJ` directory and its subdirectories – *ITM_HOME*`\logs` directory and its subdirectories For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.

Table 14. Permissions required when configuring a DB2 database (continued)

Task	User and Database Requirements
Requirements for database administrator user specified with the `ConfigDMS` utility	The requirements are as follows: • The user must be a DB2 administrator user (for example, *db2admin*). Alternatively, the user can be a database user specific to the database with at least the following authorizations: – Connect to the database – Create tables – Perform select, insert, update, and delete operations on the tables in the database The user is used by the SOA Domain Management Server or Tivoli Common Object Repository to access the database at run time. The SOA Domain Management Server user name is not to be used as the database schema name. The schema name is hard-coded to *SDMS*. The Tivoli Common Object Repository user name is used as the database schema name.

Microsoft SQL Server database configuration permissions

The permissions that are required when configuring a Microsoft SQL Server database for SOA Domain Management Server as part of an installation of ITCAM for SOA are in Table 15:

Table 15. Permissions required when configuring a Microsoft SQL Server database

Task	User and Database Requirements
Configuring Microsoft SQL Server	Authentication mode for the SQL server must be configured for mixed mode (Windows authentication and SQL Server authentication). With mixed mode authentication, both Windows authentication and Microsoft SQL Server authentication are enabled.
Permissions required to run the `kd4MakeMSSQLdb.bat` script to manually create a Microsoft SQL Server database either locally or remotely	The requirements are as follows: • The user must run the `kd4MakeMSSQLdb.bat` script as a user that is a member of the SQL Server `sysadmin` role group. • The user must have read, write, and execute permissions for the directory *`ITM_HOME`*`\CNPS\Products\KD4\latest\bin` where the `kd4MakeMSSQLdb.bat` script it located.

Table 15. Permissions required when configuring a Microsoft SQL Server database (continued)

Task	User and Database Requirements
Permissions required to run the ConfigDMS utility to either (a) configure a Microsoft SQL Server database that was created locally or remotely, or (b) create the Microsoft SQL Server database locally and configure it	When creating the database in the ConfigDMS utility, the requirements are as follows: • User must run the ConfigDMS utility as a user that is a member of the SQL Server sysadmin role group to create the database. • User must have read, write, and modify permissions for the following directories: – *ITM_HOME*\CNPS directory and its subdirectories – *ITM_HOME*\CNPSJ directory and its subdirectories – *ITM_HOME*\logs directory and its subdirectories When the database is created already, the requirements are as follows: • The user must have Windows administrator privileges (for example, in Administrators group). • The user must be the user who installed IBM Tivoli Monitoring. • The user must have read, write, and modify permissions for the following directories: – *ITM_HOME*\CNPS directory and its subdirectories – *ITM_HOME*\CNPSJ directory and its subdirectories – *ITM_HOME*\logs directory and its subdirectories
Requirements for database administrator user specified with the ConfigDMS utility	When creating the database with the ConfigDMS utility, the requirements are as follows: • The server login user can be any existing or non-existing user, except for the reserved user, sa. If the server login user that you specify does not exist, it is created in the SQL Server registry. The ConfigDMS utility assigns this user the db_owner role for the SOA Domain Management Server database. When the database is created already, the requirements are: • The user must be the server login user specified when the kd4MakeMSSQLdb script was run on the database server or the portal server.

Oracle database configuration permissions

The permissions that are required when configuring an Oracle database for SOA Domain Management Server and Tivoli Common Object Repository as part of an installation of ITCAM for SOA are in Table 16:

Table 16. Permissions required when configuring an Oracle database

Task	User and Database Requirements
Permissions required to run the KD4InitOracleDb.bat script	The requirements are as follows: • The user who created the SOA Domain Management Server database must have read, write, and execute permissions for the directory on the local server or the remote server that contains the KD4InitOracleDb.bat script. • The script must be run as the user who created the SOA Domain Management Server database.

Table 16. Permissions required when configuring an Oracle database (continued)

Task	User and Database Requirements
Permissions required to run the make_ora_user.bat script	The requirements are as follows: • The user who created the Tivoli Common Object Repository database must have read, write, and execute permissions for the directory on the local server or the remote server that contains the make_ora_user.bat script. • The script must be run as the user who created the Tivoli Common Object Repository database.
Requirements for database user specified when running the KD4InitOracleDb.bat script	The user name and schema are hardcoded as *SDMS*. If the user exists, it is dropped and recreated by the script.
Requirements for database user specified when running the make_ora_user.bat script	The requirements are as follows: • If the user exists, it is dropped and recreated by the script. • Do not specify *SDMS* as the user name when running the script. The user name is also used as the schema name.
Permissions required to run the ConfigDMS utility to configure an Oracle database that is configured locally or remotely	The requirements are as follows: • The user must be the user who installed IBM Tivoli Monitoring. • The user must have permission to reconfigure and run the Tivoli Enterprise Portal Server. • The user must have read, write, and modify permissions for the following directories: – *ITM_HOME*\CNPS directory and its subdirectories – *ITM_HOME*\CNPSJ directory and its subdirectories – *ITM_HOME*\logs directory and its subdirectories
Requirements for database administrator user specified with the ConfigDMS utility	The requirements for the SOA Domain Management Server are as follows: • The SOA Domain Management Server user is hard-coded to *SDMS*. • The password must be the same as the password specified when you ran the kd4InitOracleDb.bat script. The requirements for Tivoli Common Object Repository are: • The user name must be the same as the user name specified when you ran the make_ora_user.bat script.

Permissions required when upgrading to ITCAM for SOA V7.2 or updating to ITCAM for SOA V7.2 Fix Pack 1

Before you upgrade or update topology support, review the permissions required for configuring SOA Domain Management Server and Tivoli Common Object Repository local databases when performing the following tasks:

- Upgrading ITCAM for SOA from version 7.1.1 (all releases) to version 7.2.
- Migrating remote databases from version 7.1.1.3 to version 7.2.
- Updating ITCAM for SOA from version 7.2 to version 7.2 Fix Pack 1.

The permissions required are outlined in the following sections.

DB2 database upgrade and update permissions

The permissions required when migrating a DB2 database for SOA Domain Management Server and Tivoli Common Object Repository are in Table 17 on page 119:

Table 17. Permissions required when upgrading a DB2 database

Task	User and Database Requirements
Permissions required to run the `ConfigDMS` utility to upgrade a local DB2 database.	The requirements are as follows: • The user must have Windows administrator privileges (for example, in Administrators group). • The user must be the user who installed IBM Tivoli Monitoring. • The user must have read, write, and modify permissions for the following directories: – `*ITM_HOME*\CNPS` directory and its subdirectories – `*ITM_HOME*\CNPSJ` directory and its subdirectories – `*ITM_HOME*\logs` directory and its subdirectories
Permissions required to run the `kd4MigrateDB2db.bat` script to migrate a remote SOA Domain Management Server database	The requirements are as follows: • The user who created the SOA Domain Management Server database must have read, write, and execute permissions for the directory on the remote server that contains the `kd4MigrateDB2db.bat` script. • The script must be run as the user who created the SOA Domain Management Server database.

Microsoft SQL Server database upgrade and update permissions

The permissions required when upgrading or updating a Microsoft SQL Server database for SOA Domain Management Server are in Table 18:

Table 18. Permissions required when upgrading a Microsoft SQL Server database

Task	User and Database Requirements
Permissions required to run the `ConfigDMS` utility to upgrade a local Microsoft SQL Server SOA Domain Management Server database	The requirements are as follows: • The user must have Windows administrator privileges (for example, in Administrators group). • The user must be the user who installed IBM Tivoli Monitoring. • The user must have read, write, and modify permissions for the following directories: – `*ITM_HOME*\CNPS` directory and its subdirectories – `*ITM_HOME*\CNPSJ` directory and its subdirectories – `*ITM_HOME*\logs` directory and its subdirectories
Permissions required to run the `kd4MigrateMSSQLdb.bat` script to migrate a remote Microsoft SQL Server SOA Domain Management Server database	The requirements are as follows: • The user who created the SOA Domain Management Server database must have read, write, and execute permissions for the directory on the remote server that contains the `kd4MigrateMSSQLdb.bat` script. • The script must be run as the user who created the SOA Domain Management Server database.

Oracle database upgrade permissions

The permissions required when migrating an Oracle database for SOA Domain Management Server and Tivoli Common Object Repository are in Table 19 on page 120:

Table 19. Permissions required when upgrading an Oracle database

Task	User and Database Requirements
Permissions required to run the `ConfigDMS` utility to upgrade an Oracle database that is created locally	The requirements are as follows: • The user must be the user who installed IBM Tivoli Monitoring. • The user must have permission to reconfigure and run the Tivoli Enterprise Portal Server. • The user must have read, write, and modify permissions for the following directories: – `ITM_HOME\CNPS` directory and its subdirectories – `ITM_HOME\CNPSJ` directory and its subdirectories – `ITM_HOME\logs` directory and its subdirectories For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
Permissions required to run the `kd4MigrateOracledb.bat` script to migrate a remote Oracle SOA Domain Management Server database	The requirements are as follows: • The user who created the SOA Domain Management Server database must have read, write, and execute permissions for the directory on the remote server that contains the `kd4MigrateOracledb.bat` script. • The script must be run as the user who created the SOA Domain Management Server database.

Considerations when configuring SOA Domain Management Server and Tivoli Common Object Repository together

If you are using the `ConfigDMS` utility to configure both SOA Domain Management Server and Tivoli Common Object Repository, you must be signed in as a user that has the permissions for configuring both components.

In the special case in which you configure topology support with SOA Domain Management Server in Microsoft SQL Server and Tivoli Common Object Repository on a local DB2 server, you must sign in with a user name that has appropriate database administrator privileges for both the Microsoft SQL Server and the DB2 database. In this case, you configure both SOA Domain Management Server and Tivoli Common Object Repository in a single run of the `ConfigDMS` utility. You must also run the `ConfigDMS` utility from a DB2 command line processor window.

If you do not have a single user with the appropriate permissions, you must sign in twice to run the `ConfigDMS` utility:

- Signing in the first time: Sign in with a user name that has permissions to run the `ConfigDMS` utility to configure only SOA Domain Management Server. After this task completes successfully, you must reconfigure Tivoli Enterprise Portal Server before proceeding.
- Signing in the second time: Sign in a second time with a user name that has permissions to run the `ConfigDMS` utility to configure Tivoli Common Object Repository. After this task completes successfully, you must reconfigure Tivoli Enterprise Portal Server and then start the portal server.

Creating the SOA Domain Management Server database

The SOA Domain Management Server database can be created on a supported DB2 server, Microsoft SQL server, or Oracle server.

When creating the SOA Domain Management Server database, you have the following options:

- Let the SOA Domain Management Server Configuration utility create and configure the SOA Domain Management Server database locally for you on your portal server computer.
- Manually create a database on the local portal server before running the SOA Domain Management Server Configuration utility.
- Manually create a database on a remote database server before running the SOA Domain Management Server Configuration utility.

Restriction: If an Oracle database is used for the SOA Domain Management Server, it must be created manually before running the SOA Domain Management Server Configuration utility.

If this database server is installed on the same computer as the portal server, the database server is usually the same database server that is used by the portal server.

Manually creating a local SOA Domain Management Server database

To create and configure the SOA Domain Management Server database locally, use the scripts in the `*TEPS_Home*\Products\KD4\latest\bin` directory on the computer where the portal server is installed.

You can use either a DB2, Microsoft SQL Server, or Oracle database to create the SOA Domain Management Server database.

When the database is created or installed locally with the scripts provided, you must run the `ConfigDMS` utility to configure the database. From the `ConfigDMS` utility, choose the option to use an existing database. When the database is configured, you must reconfigure and restart the Tivoli Enterprise Portal Server.

Manually creating a DB2 database locally on Windows systems for SOA Domain Management Server

To manually create the DB2 database locally, complete these steps:

1. Verify that your user name has Windows and DB2 administrative privileges on the local computer. (For example, a user in the Administrators and DB2ADMNS groups.)
2. Open a DB2 command line processor window. Click **Start** > **Run** and enter the **`db2cmd`** command.
3. In the DB2 command line processor window, navigate to the `*ITM_Home*\CNPS\Products\KD4\latest\bin` directory.

   For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.
4. Verify that your user name has permission to read and run the `kd4MakeDB2db.bat` script and write permission for the directory that contains the script.
5. Run the `kd4MakeDB2db.bat` script and provide a name for the SOA Domain Management Server database, such as `KD4SDMS`. The name can have a maximum of 8 characters. For example:

   ```
   kd4MakeDB2db KD4SDMS
   ```

Tip: If this database exists on the local system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.

6. Wait for the database creation process to complete.

   The script verifies the database version and displays a message if the version is unsupported. The output that is generated by this script is written to a file called `createDB2DBResults.txt` in the same directory where the script is run. See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with any errors that you encounter.
7. Close the DB2 command-line window.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 115.

Manually creating a Microsoft SQL Server database locally on Windows systems for SOA Domain Management Server

To run the script on the local computer for Microsoft SQL Server, complete these steps:

1. Verify that your user name has appropriate Windows and Microsoft SQL Server database permissions.

   To create the SOA Domain Management Server database with Microsoft SQL Server, the Authentication mode for the SQL server must be configured for Mixed Mode (Windows Authentication and SQL Server Authentication). When using Microsoft SQL Server Authentication, a user that logs in to Microsoft SQL Server must supply a user name and a password that Microsoft SQL Server validates against a system table. With this security model, log in as a user that is a member of the SQL Server `sysadmin` role group to create the SOA Domain Management Server database.
2. Open a command prompt window.
3. Navigate to the *ITM_Home*`\CNPS\Products\KD4\latest\bin` directory.

   For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.

   Verify that your user has read, write, and execute permissions for this directory.
4. Run the `kd4MakeMSSQLdb.bat` script by following this syntax:

   ```
   kd4MakeMSSQLdb dbname dbuser
   dbpassword dbtype [dbInstance]
   ```

   Where:

   dbname

   Specifies the SOA Domain Management Server database name, for example, `KD4SDMS`. The name can have a maximum of 128 characters.

   Tip: If this database exists on the local system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.

   dbuser Specifies the Microsoft SQL Server database server login name, for example, *sdms*. This name can be any existing or non-existing user, except for the reserved user name, *sa*. If the name that you specify does not exist, it is created in the Microsoft SQL Server registry. The user is granted the *db_owner* role for the database.

   dbpassword

   Specifies the database password for the specified user *dbuser*.

dbtype Specifies the version of your Microsoft SQL Server installation. The only valid value is `MSSQL2005`.

Important: To specify a Microsoft SQL Server 2008 installation, use `MSSQL2005`.

dbInstance
(Optional) Specifies a named instance of Microsoft SQL Server, in the form of `database_hostname\instance_name`. The value *database_hostname* is the name of the computer where the database server is installed. The value *instance_name* is the instance name, for example, `localhost\MyInstance`. If no value is specified, the default instance is assumed.

5. Wait for the database creation process to complete.

   The script verifies the database version and displays a message if the version is unsupported.

   The output that is generated by this script is written to a file called `createMSSQLDBResults.txt` in the same directory where the script is run.
6. Close the command prompt window.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 115.

Manually creating an Oracle database locally on Windows systems for SOA Domain Management Server

The Oracle database that you use for SOA Domain Management Server must meet these requirements:

- The Oracle database must be created with Unicode (AL32UTF8) as the database character set.
- The Oracle database must be created with UTF8 as the national character set.

To manually create the Oracle database locally, complete these steps:

1. Install Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 on the portal server.
2. Use the Database Configuration Assistant (DBCA) to create a database locally for the SOA Domain Management Server. For specific instructions on how to create the Oracle database, refer to your Oracle database documentation.
3. Ensure that you are logged in as the user who created the Oracle database for the SOA Domain Management Server.
4. Start the Oracle listener with the Oracle Listener Service.
5. Navigate to the *ITM_Home*`\CNPS\Products\KD4\latest\bin` directory. Verify that your user name has permission to read and issue the `kd4InitOracleDb.bat` script, the `kd4InitOracleDB_user.sql` file, and the `sdms_oracle.sql` file. Verify that your user name has write permission for that directory.
6. Run the `kd4InitOracleDb.bat` script to create the SOA Domain Management Server user, create the SOA Domain Management Server role, grant authorities, and create the schema. The name of the Oracle user and the name of the schema is hardcoded as *SDMS*. Use this syntax:

```
kd4InitOracleDb.bat SID ORACLE_HOME USER_PW SYS_PW
```

   Where:

   SID Specifies the Oracle System Identifier (SID) for the SOA Domain Management Server database.

ORACLE_HOME

Specifies the directory where the Oracle database server is installed, for example, `C:\app\Administrator\product\11.1.0\db_1`.

If the `ORACLE_HOME` environment variable is set, you can provide it as the value for this parameter.

Tip: Ensure that the directory path does not end with a backslash (\).

USER_PW

Specifies the password for the Oracle SOA Domain Management Server user created by the `kd4InitOracleDb.bat` script.

SYS_PW

Specifies the password for the *SYS* user.
The *SYS* user is created automatically when you create an Oracle database.

7. Wait for the `kd4InitOracleDb.bat` script to complete.

   Remember: If an Oracle user called SDMS exists, it can take some time to drop the user and re-create it. During this time, the script can seem to hang.
8. Close the command prompt window.

The results of the `Kd4InitOracleDb.bat` script are written to the `initOracleDBresults.txt` file.

If errors occur while running the `Kd4InitOracleDb.bat` script, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more details.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 115.

Manually creating a remote SOA Domain Management Server database

To create and configure the SOA Domain Management Server DB2, Microsoft SQL Server, or Oracle database on a remote server, copy the `kd4RemoteDB.zip` file from the *TEPS_Home*`/Products/KD4/latest/db` directory (on the computer where your portal server is installed) to the remote computer where you plan to create the SOA Domain Management Server database. Extract this file into any directory and run the provided scripts to create the database as needed.

Restriction: The `kd4RemoteDB.zip` file is only available after ITCAM for SOA application support is installed.

When the database is created or installed remotely with the scripts, you must run the `ConfigDMS` utility with the `-remoteSDMS` argument to configure the database. From the `ConfigDMS` utility, choose the option to use an existing database. When the database is configured, you must reconfigure and restart the Tivoli Enterprise Portal Server.

Manually creating a DB2 database remotely on Windows systems for SOA Domain Management Server

To manually create a DB2 database on a remote server, complete these steps:

1. Verify that your user name has Windows and DB2 administrative privileges on the remote computer. (For example, the user name must be included in the Administrators and DB2ADMNS groups).

2. Open a DB2 command line processor window. Click **Start** > **Run** and enter the **db2cmd** command.
3. In the DB2 command line processor window, navigate to the directory where you copied the kd4MakeDB2db.bat script.
4. Verify that your user name has permission to read and run the kd4MakeDB2db.bat script and write permission for the directory that contains the script.
5. Run the kd4MakeDB2db.bat script and provide a name for the SOA Domain Management Server database, such as KD4SDMS. The name can have a maximum of 8 characters. For example:

   ```
   kd4MakeDB2db KD4SDMS
   ```

   Remember: If this database exists on the remote system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.
6. Wait for the database creation process to complete.

   The script verifies the database version and displays a message if it is at an unsupported level. The output generated by this script is written to a file called createDB2DBResults.txt in the same directory where the script is run. See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with any errors that you might encounter.
7. Close the DB2 command-line window.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 115.

Manually creating a Microsoft SQL Server database remotely on Windows systems for SOA Domain Management Server

To run the script on the remote computer for Microsoft SQL Server, complete these steps:

1. Verify that your user name has Windows and Microsoft SQL Server administrative privileges (typically a user in the Windows Administrators group).

   To create the SOA Domain Management Server database with Microsoft SQL Server, the Authentication mode for the SQL server must be configured for Mixed Mode (Windows Authentication and SQL Server Authentication). When using Microsoft SQL Server Authentication, a user that logs in to Microsoft SQL Server must supply a user name and a password that Microsoft SQL Server validates against a system table. With this security model, log in as a user that is a member of the SQL Server sysadmin role group to create the SOA Domain Management Server database.
2. Open a command prompt.
3. Navigate to the directory where you copied the kd4MakeMSSQLdb.bat script.
4. Run the kd4MakeMSSQLdb.bat script with this syntax:

   ```
   kd4MakeMSSQLdb dbname dbuser
   dbpassword dbtype [dbInstance]
   ```

   Where:

   dbname

   Specifies the SOA Domain Management Server database name, for example, KD4SDMS. The name can have a maximum of 128 characters.

Remember: If this database exists on the remote system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.

dbuser Specifies the Microsoft SQL Server database server login name, for example, *sdms*. This name can be any existing or non-existing user, except for the reserved user name, *sa*. If the name that you specify does not exist, it is created in the Microsoft SQL Server registry. This user is granted the *db_owner* role for the database.

dbpassword
Specifies the database password for the specified user *dbuser*.

dbtype Specifies the version of your Microsoft SQL Server installation. The only valid value is `MSSQL2005`.

Tip: To specify a Microsoft SQL Server 2008 installation, use `MSSQL2005`.

dbInstance
(Optional) Specifies a named instance of Microsoft SQL Server, in the form of *`database_hostname\instance_name`*. The value *database_hostname* is the name of the computer where the database server is installed. The value *instance_name* is the instance name, for example, *`localhost\MyInstance`*. If no value is specified, the default instance is assumed.

5. Wait for the database creation process to complete.

   The script verifies the database version and displays a message if it is at an unsupported level.

   The output generated by this script is written to a file called `createMSSQLDBResults.txt` in the same directory where the script is run.
6. Close the command prompt window.

For information about database and user permissions when creating and configuring topology databases, see “Database and User Permissions” on page 115.

Manually creating an Oracle database remotely on Windows systems for SOA Domain Management Server

The Oracle database that you use for SOA Domain Management Server must meet these requirements:

- The Oracle database must be created with Unicode (AL32UTF8) as the database character set.
- The Oracle database must be created with UTF8 as the national character set.

To manually create the Oracle database on a remote server, complete these steps:

1. Install Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 on the remote server
2. Use the Database Configuration Assistant (DBCA) to create a database on the remote server for the SOA Domain Management Server.
   For specific instructions on how to create the Oracle database, refer to your Oracle database documentation.
3. Ensure that you are logged in as the user who created the Oracle database for the SOA Domain Management Server.
4. Start the Oracle listener with the Oracle Listener Service.
5. Navigate to the directory on the remote computer where you extracted the `kd4RemoteDB.zip`. Verify that your user name has permission to read and issue

the kd4InitOracleDb.bat script, the kd4InitOracleDB_user.sql file, and the sdms_oracle.sql file. Verify that your user name has write permission for that directory.

6. Run the kd4InitOracleDb.bat script to create the SOA Domain Management Server user, create the SOA Domain Management Server role, grant authorities, and create the schema. The name of the Oracle user and the name of the schema is hard-coded as *SDMS*. Use this syntax:

   ```
   kd4InitOracleDb.bat  SID ORACLE_HOME USER_PW SYS_PW
   ```

   Where:

   SID Specifies the Oracle System Identifier (SID) for the SOA Domain Management Server database.

   ORACLE_HOME
   Specifies the directory where the Oracle database server is installed, for example, C:\app\Administrator\product\11.1.0\db_1.

   If the ORACLE_HOME environment variable is set, you can provide it as the value for this parameter.

   Tip: Ensure that the directory path does not end with a backslash (\).

   USER_PW
   Specifies the password for the Oracle SOA Domain Management Server user created by the kd4InitOracleDb.bat script.

   SYS_PW
   Specifies the password for the SYS user.
   The SYS user is created automatically when you create an Oracle database.

7. Wait for the kd4InitOracleDb.bat script to complete.

   Remember: If an Oracle user called SDMS exists, it can take some time to drop the user and re-create it. During this time, the script can appear to hang.

If errors occur while running the Kd4InitOracleDb.bat script, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more details.

For information about database and user permissions when creating and configuring topology databases, see “Database and User Permissions” on page 115.

Creating the Tivoli Common Object Repository database

The Tivoli Common Object Repository database can be created on a supported DB2 server or Oracle server.

When creating the Tivoli Common Object Repository database, you have the following options:

- Let the SOA Domain Management Server Configuration utility create and configure the Tivoli Common Object Repository database locally for you on your portal server computer.
- Manually create a database on the local portal server before running the SOA Domain Management Server Configuration utility.
- Manually create a database on a remote database server before running the SOA Domain Management Server Configuration utility.

Restriction: If an Oracle database is used for the Tivoli Common Object Repository, it must be created manually before running the SOA Domain Management Server Configuration utility.

If this database server is installed on the same computer as the portal server, the database server is usually the same database server that is used by the portal server.

Manually creating a local Tivoli Common Object Repository database

To create and configure the Tivoli Common Object Repository DB2 database locally, use the `make_db2_db.bat` script found in the *TEPS_Home*`/Products/KD4/latest/tcore/db` directory on the computer where the portal server is installed.

Important: This script creates the Tivoli Common Object Repository database but does not create the database schema or tables. The schema and tables are created when you run the SOA Domain Management Server Configuration utility to configure Tivoli Common Object Repository.

To configure an Oracle database for Tivoli Common Object Repository, manually create the database with the Oracle Database Configuration Assistant and use the `make_ora_user.bat` found in the *TEPS_Home*`/Products/KD4/latest/tcore/db` directory to create user roles and grant authorities.

When the database is created or installed locally with the scripts provided, you must run the `ConfigDMS` utility to configure the database. From the `ConfigDMS` utility, choose the option to use an existing database. When the database is configured, you must reconfigure and restart the Tivoli Enterprise Portal Server.

Manually creating a DB2 database locally on Windows systems for Tivoli Common Object Repository

To manually create the DB2 database locally, complete these steps:

1. Verify that your user name has Windows and DB2 administrative privileges.
2. Open a DB2 command line processor window. Click **Start** > **Run** and enter the **`db2cmd`** command.
3. In the DB2 command line processor window, navigate to the *ITM_Home*`\CNPS\Products\KD4\latest\tcore\db` directory. Verify that the user has read and run permission for the `make_db2_db.bat` script in this directory.

   For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
4. Run the `make_db2_db.bat` script and provide a name for the Tivoli Common Object Repository database, such as `KD4TCORE`.

   The name can have a maximum of eight characters. For example:

   ```
   make_db2_db KD4TCORE
   ```

   Remember: If this database exists on the local system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.
5. Wait for the database creation process to complete.

   See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with any errors that you might encounter.
6. Close the DB2 command line processor window.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 115.

Manually creating an Oracle database locally on Windows systems for Tivoli Common Object Repository

The database that you use for Tivoli Common Object Repository must meet these requirements:

- The Oracle database must be created with Unicode (AL32UTF8) as the database character set.
- The Oracle database must be created with UTF8 as the national character set.

Important: If you use an Oracle database for Tivoli Common Object Repository, it is recommended that you also use an Oracle database for SOA Domain Management Server.

To manually create the Oracle database locally, complete these steps:

1. Install Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 on the portal server.
2. Use the Database Configuration Assistant (DBCA) to create a database locally for the Tivoli Common Object Repository.
   For specific instructions on how to create the Oracle database, refer to your Oracle database documentation.
3. Ensure that you are logged in as the user who created the Oracle database for the Tivoli Common Object Repository.
4. Ensure the ORACLE_HOME environment variable is set to the directory where your Oracle database server is installed.
5. Start the Oracle listener using the Oracle Listener Service.
6. Navigate to the *ITM_Home*\CNPS\Products\KD4\latest\tcore\db directory and verify that your user has read, write, and execute permissions for this directory.

   For more information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
7. Run the make_ora_user.bat script to create the Tivoli Common Object Repository user, create the Tivoli Common Object Repository role, grant authorities, and create the schema. The name of the Oracle user and the name of the schema is hardcoded as TCORE. Use this syntax:

   ```
   make_ora_user.bat SID USER_NAME USER_PW
   ```

   Where:

   SID Specifies the Oracle System Identifier (SID) for the Tivoli Common Object Repository database.

   USER_NAME
   Specifies the name of the Oracle user that is created by the make_ora_user.bat script.

   Tip: Do not specify SDMS as the user name when running the script.

   USER_PW
   Specifies the password for the Oracle Tivoli Common Object Repository user created by the script.

   Important: The make_ora_user.bat script also accepts optional parameters for the archive user name and password. You must not enter these parameter values when configuring Tivoli Common Object Repository.

8. Wait for the `make_ora_user.bat` script to complete.

If errors occur while running the `make_ora_user.bat` script, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more details.

For information about database and user permissions when creating and configuring topology databases, see “Database and User Permissions” on page 115.

Manually creating a remote Tivoli Common Object Repository database

To create and configure the Tivoli Common Object Repository DB2 database remotely, copy the `make_db2_db.bat` script found in the *TEPS_Home*`/Products/KD4/latest/tcore/db` directory (on the computer where your Tivoli Enterprise Portal Server is installed) to the remote computer where you plan to create the Tivoli Common Object Repository database, and run this script to create the database.

Important: This script creates the Tivoli Common Object Repository database but does not create the database schema or tables. The schema and tables are created when you run the SOA Domain Management Server Configuration utility to configure Tivoli Common Object Repository.

To configure an Oracle database for Tivoli Common Object Repository remotely, manually create the database with the Oracle Database Configuration Assistant on the remote computer. Copy the `make_ora_user.bat` script found in the *TEPS_Home*`/Products/KD4/latest/tcore/db` directory to the remote computer where you plan to create the Tivoli Common Object Repository database, and run this script to create user roles and grant authorities.

When the database is created or installed remotely with the scripts provided, you must run the `ConfigDMS` utility with the `-remoteTCORE` argument to configure the database. From the `ConfigDMS` utility, choose the option to use an existing database. When the database is configured, you must reconfigure and restart the Tivoli Enterprise Portal Server.

Manually creating a DB2 database remotely on Windows systems for Tivoli Common Object Repository

To run the script on the remote computer for DB2, complete these steps:

1. Verify that your user name has Windows and DB2 administrative privileges on the remote computer (for example, the user name must be included in the Administrators and DB2ADMNS groups).
2. Open a DB2 command line processor window. Click **Start** > **Run** and enter the **`db2cmd`** command.
3. In the DB2 command line processor window, navigate to the directory where you copied the `make_db2_db.bat` script.

   Verify that your user has read and execute permission for the `make_db2_db.bat` script in this directory.
4. Run the `make_db2_db.bat` script and provide a name for the Tivoli Common Object Repository database, such as `KD4TCORE`.

   The name can have a maximum of 8 characters. For example:

   ```
   make_db2_db KD4TCORE
   ```

   Remember: If this database exists on the remote system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.

5. Wait for the database creation process to complete.

   See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with any errors that you might encounter.
6. Close the DB2 command line processor window.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 115.

Manually creating an Oracle database remotely on Windows systems for Tivoli Common Object Repository

The database that you use for Tivoli Common Object Repository must meet these requirements:

- The Oracle database must be created with Unicode (AL32UTF8) as the database character set.
- The Oracle database must be created with UTF8 as the national character set.

Important: If you use an Oracle database for Tivoli Common Object Repository, it is recommended that you also use an Oracle database for SOA Domain Management Server.

To manually create the Oracle database on a remote server, complete these steps:

1. Install Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 on the remote server.
2. Use the Database Configuration Assistant (DBCA) to create a database remotely for the Tivoli Common Object Repository.
   For specific instructions on how to create the Oracle database, refer to your Oracle database documentation.
3. Ensure that you are logged in as the user who created the Oracle database for the Tivoli Common Object Repository.
4. Ensure the `ORACLE_HOME` environment variable is set to the directory where your Oracle database server is installed.
5. Start the Oracle listener with the Oracle Listener Service.
6. Navigate to the directory on the remote computer where you copied the `make_ora_user.bat` script. Verify that your user has read, write, and execute permissions for this directory.
7. Run the `make_ora_user.bat` script to create the Tivoli Common Object Repository user, create the Tivoli Common Object Repository role, grant authorities, and create the schema. The name of the Oracle user and the name of the schema is hardcoded as `TCORE`. Use this syntax:

   ```
   make_ora_user.bat SID USER_NAME USER_PW
   ```

   Where:

   SID Specifies the Oracle System Identifier (SID) for the Tivoli Common Object Repository database.

   USER_NAME
   Specifies the name of the Oracle user that is created by the script `make_ora_user.bat`.

   Tip: Do not specify `SDMS` as the user name when running the script.

   USER_PW
   Specifies the password for the Oracle Tivoli Common Object Repository user created by the script.

Important: The make_ora_user.bat script also accepts optional parameters for the archive user name and password. You must not enter these parameter values when configuring Tivoli Common Object Repository.

8. Wait for the make_ora_user.bat script to complete.

If errors occur while running the make_ora_user.bat script, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more details.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 115.

Running the ConfigDMS utility

ITCAM for SOA provides the SOA Domain Management Server Configuration utility (referred to as ConfigDMS) that simplifies the configuration of SOA Domain Management Server and Tivoli Common Object Repository topology support. The utility runs in either a graphical user interface mode or in console mode. A silent configuration method is also supported, and optional logging controls are provided to help you diagnose problems.

In addition to configuring topology support, you can use the ConfigDMS utility to create SOA Domain Management Server and Tivoli Common Object Repository DB2 or Microsoft SQL Server databases locally.

If preferred, you can use the database creation scripts provided with the product to create local or remote databases.

Restriction: If you are using Oracle databases, you cannot use the ConfigDMS utility to create the databases. You must create the databases using the database creation scripts provided with the product before running the utility.

For information about the procedures for creating these databases before running the utility, see "Creating the SOA Domain Management Server database" on page 120 and "Creating the Tivoli Common Object Repository database" on page 127.

Installation tasks

You can use the utility to complete any of the following installation tasks:

- If you are performing a fresh installation of ITCAM for SOA version 7.2 fix pack 1, use the SOA Domain Management Server Configuration utility to configure SOA Domain Management Server and optionally configure Tivoli Common Object Repository.
- If you configured SOA Domain Management Server for ITCAM for SOA version 7.2 fix pack 1 but not Tivoli Common Object Repository, you can use the SOA Domain Management Server Configuration utility to configure Tivoli Common Object Repository at a later point.

Upgrade and update tasks

You can use the utility to complete any of the following upgrade and update tasks:

- If you are upgrading from ITCAM for SOA version 7.1.1, you use the SOA Domain Management Server Configuration utility to upgrade SOA Domain Management Server and Tivoli Common Object Repository (if it is configured).

- When you are updating from ITCAM for SOA version 7.2 to version 7.2 fix pack 1, use the SOA Domain Management Server Configuration utility to update SOA Domain Management Server and Tivoli Common Object Repository (if it is configured).
- If you are upgrading or updating a remote SOA Domain Management Server Configuration utility database, you must also run a migration script to migrate the database. For more information, see "Upgrading a previous topology configured remotely" on page 144.

Remember: When you are upgrading from ITCAM for SOA version 7.1.1, you must upgrade topology support to version 7.2 before you update topology support to 7.2 fix pack 1.

Authentication tasks

You can use the utility to complete any of the following authentication tasks:

- If your SOA Domain Management Server database password changed, you use the SOA Domain Management Server Configuration utility to update the database password used to access the SOA Domain Management Server database.
- If your Tivoli Common Object Repository database password changed, you use the SOA Domain Management Server Configuration utility to update the database password used to access the Tivoli Common Object Repository database.

Upgrading from a previous version

You must upgrade from ITCAM for SOA version 7.1.1 (all releases) to ITCAM for SOA version 7.2 before you update the agent to ITCAM for SOA version 7.2 Fix Pack 1.

Upgrading from ITCAM for SOA V7.1.1 (all releases) to V7.2

When you upgrade from a previous ITCAM for SOA version 7.1.1 (all releases) installation to a 7.2 installation, you run the SOA Domain Management Server Configuration utility (`ConfigDMS`) to upgrade the configuration for SOA Domain Management Server, and optionally, for Tivoli Common Object Repository, if it exists. In version 7.1.1 (all releases), the Tivoli Common Object Repository component is optional. The `ConfigDMS` utility automatically detects whether Tivoli Common Object Repository is configured, and performs the upgrade.

Important: Before you upgrade to ITCAM for SOA version 7.2, you must verify that the databases you use for SOA Domain Management Server or Tivoli Common Object Repository are at one of the minimum supported levels. For information about the supported versions of the databases, see the prerequisites for ITCAM for SOA from the Software product compatibility reports website. For more information about accessing these reports, see "Required software" on page 15.

Upgrading SOA Domain Management Server

The `ConfigDMS` utility automatically upgrades the SOA Domain Management Server component. If your SOA Domain Management Server version 7.1.1 database resides on a remote system, you must use the `ConfigDMS` utility with the argument `-remoteSDMS` to upgrade ITCAM for SOA support for the databases to version 7.2 and manually migrate the SOA Domain Management Server database schema on the remote system to version 7.2.

If your database was created with Microsoft SQL Server 2000 in version 7.1.1, your database administrator must manually migrate the Microsoft SQL Server database to a supported database version (Microsoft SQL Server 2005 or Microsoft SQL Server 2008).

Upgrading Tivoli Common Object Repository

The SOA Domain Management Server Configuration utility automatically upgrades the Tivoli Common Object Repository component to the version 7.2 level if it is configured. User credentials and properties are preserved during the upgrade. User settings in properties files, such as the `collation.properties` and the `bulkload.properties` files, are also preserved. If your Tivoli Common Object Repository version 7.1.1 database resides on a remote system, you must use the `ConfigDMS` utility with the argument `-remoteTCORE` to upgrade ITCAM for SOA support for the databases to version 7.2.

When you upgrade both SOA Domain Management Server and Tivoli Common Object Repository from a previous ITCAM for SOA version 7.1.1 (all releases) configuration to a version 7.2 configuration, SOA Domain Management Server is upgraded first, and then the upgrade of Tivoli Common Object Repository occurs automatically (you are not first prompted to continue with the upgrade of Tivoli Common Object Repository). If either part of this upgrade process does not complete successfully, an error message is displayed. You must resolve the problem and then run the `ConfigDMS` utility again.

Updating from ITCAM for SOA V7.2 to version V7.2 Fix Pack 1

When you update topology support from ITCAM for SOA 7.2 to ITCAM for SOA version 7.2 Fix Pack 1, the procedure to follow is the same as the procedure for upgrading from ITCAM for SOA 7.1.1 (all releases) to ITCAM for SOA version 7.2.

To update topology support from ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1, run the `ConfigDMS` utility to update the configuration for SOA Domain Management Server, and optionally, for Tivoli Common Object Repository, if it exists. The `ConfigDMS` utility automatically detects whether Tivoli Common Object Repository is configured, and performs the update.

Updating SOA Domain Management Server

The `ConfigDMS` utility automatically updates the SOA Domain Management Server component. If your SOA Domain Management Server version 7.2 database resides on a remote system, you must use the `ConfigDMS` utility with the argument `-remoteSDMS` to perform the following activities:

- Update ITCAM for SOA support for the databases to version 7.2 Fix Pack 1
- Migrate the SOA Domain Management Server database schema on the remote system to version 7.2.

Updating Tivoli Common Object Repository

The `ConfigDMS` utility automatically updates the Tivoli Common Object Repository component to the version 7.2 Fix Pack 1 level if it is configured. User credentials and properties are preserved during the update. User settings in properties files, such as the `collation.properties` and the `bulkload.properties` files, are also preserved.

If your Tivoli Common Object Repository version 7.2 database resides on a remote system, you must use the `ConfigDMS` utility with the argument `-remoteTCORE` to upgrade ITCAM for SOA support for the databases to version 7.2 Fix Pack 1.

When you upgrade both SOA Domain Management Server and Tivoli Common Object Repository from a previous ITCAM for SOA version 7.2 configuration to a version 7.2 Fix Pack 1 configuration, SOA Domain Management Server is updated first, and then the update of Tivoli Common Object Repository occurs automatically. If either part of this update process does not complete successfully, an error message is displayed. You must resolve the problem and then run the `ConfigDMS` utility again.

Upgrading and updating in silent mode

The *upgrade* property in the silent configuration file specifies whether to upgrade or update a previous configuration of both SOA Domain Management Server and Tivoli Common Object Repository, depending on already configured components:

- If only SOA Domain Management Server version 7.1.1 is configured, SOA Domain Management Server is upgraded to version 7.2.
- If SOA Domain Management Server and Tivoli Common Object Repository version 7.1.1 is configured, both are upgraded to version 7.2.
- If only SOA Domain Management Server version 7.2 is configured, SOA Domain Management Server is updated to version 7.2 Fix Pack 1.
- If SOA Domain Management Server and Tivoli Common Object Repository version 7.2 is configured, both are updated to version 7.2 Fix Pack 1.

For information about the silent response file properties that you need to specify while upgrading in silent mode, see “Running the `ConfigDMS` utility in silent mode” on page 164.

Launching the `ConfigDMS` utility

To run the `ConfigDMS` utility, complete the following steps on the local Windows computer system where Tivoli Enterprise Portal Server is installed:

1. Verify that you are logged in with a user that has the appropriate permissions as described in “Database and User Permissions” on page 115.
2. Open either a DB2 command line processor or a command prompt window.
   - Use a DB2 command line processor under the following conditions:
     - You are creating and configuring a DB2 database for the first time for the SOA Domain Management Server or Tivoli Common Object Repository with the `ConfigDMS`.
     - You are upgrading ITCAM for SOA version 7.1.1 to version 7.2. You are using DB2 for the SOA Domain Management Server database.
     - You are updating ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1. You are using DB2 for the SOA Domain Management Server database.
     - You are creating and configuring a DB2 database for Tivoli Common Object Repository but you are configuring the SOA Domain Management Server to use an Microsoft SQL Server in the same run of the SOA Domain Management Server Configuration utility.

     To open a DB2 command line processor, select **Start** > **Run** and entering **`db2cmd`**.
   - Use a command prompt under the following conditions:

- You are using the `ConfigDMS` utility to create a local SOA Domain Management Server database in Microsoft SQL Server and, optionally, you are using the utility to create a local Tivoli Common Object Repository database in Microsoft SQL Server.
- You are using the `ConfigDMS` utility to configure SOA Domain Management Server and optionally Tivoli Common Object Repository, and the databases were previously been created manually.
- You are using the `ConfigDMS` utility to upgrade from ITCAM for SOA version 7.1.1 to version 7.2, and SOA Domain Management Server is using a Microsoft SQL Server or an Oracle database.
- You are using the `ConfigDMS` utility to update from ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1, and SOA Domain Management Server is using a Microsoft SQL Server or an Oracle database.
- You are using the `ConfigDMS` utility to update the authentication parameters for the SOA Domain Management Server or Tivoli Common Object Repository database.

To open a command prompt, select **Start**>**All Programs** > **Accessories** > **Command Prompt**.

3. If you are using the `ConfigDMS` utility to upgrade from ITCAM for SOA version 7.1.1 to version 7.2 or to update from version 7.2 to version 7.2 Fix Pack 1, and the SOA Domain Management Server is using an Oracle database, complete the following steps:
   a. Verify that the `PATH` system variable in your environment variables contains the Oracle `bin` directory where `sqlplus.exe` is located. For example, `PATH=%PATH%;C:\app\Administrator\product\11.2.0\dbhome_1\bin`.
   b. Set the `ORACLE_SID` environment variable to the name of the SOA Domain Management Server database. For example, `set ORACLE_SID=KD4SDMS`.

      Important: On a computer system that has multiple installations of ITCAM for SOA, ensure that the database name specified in *ORACLE_SID* is the name of the database that is being upgraded.
   c. Set the `ORACLE_HOME` environment variable to the directory where the Oracle database server is installed, for example, `set ORACLE_HOME=C:\app\Administrator\product\11.2.0\db_1`
4. Depending on your intended task, you must run the `ConfigDMS` utility from one of two possible locations.
   - Navigate to the *`ITM_Home`*`\CNPS\Products\KD4\latest\bin` directory if any of the following conditions apply:
     - You are initially running the `ConfigDMS` utility to configure the SOA Domain Management Server or Tivoli Common Object Repository for the first time.
     - You are running the `ConfigDMS` utility to *upgrade* or *update* from a previous configuration.

     For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.
   - Navigate to the *`ITM_Home`*`\CNPS\Products\KD4\bin` directory if the following conditions apply:
     - You configured or upgraded SOA Domain Management Server and Tivoli Common Object Repository to the version 7.2 level.
     - You updated SOA Domain Management Server and Tivoli Common Object Repository to the version 7.2 Fix Pack 1 level.

- You are now running the SOA Domain Management Server Configuration utility again to *update the authentication* to access databases.

5. Run the `ConfigDMS.bat` script. This script provides several command options, described by the following syntax:

   ```
   ConfigDMS.bat [-console | -silent {silent_file}] [-debug {debug_file}]
   [-remoteSDMS] [-remoteTCORE]
   ```

   For example, to run the configuration utility with the Install Shield graphical user interface wizard, run the script without the **–console** or **–silent** options:

   ```
   ConfigDMS
   ```

   To run the configuration utility in console mode, specify the script with the **–console** option:

   ```
   ConfigDMS -console
   ```

   Important: When you are installing ITCAM for SOA, do not run the `ConfigDMS` utility as the DB2 administrator user.

These command options are described further in "ConfigDMS command options"

ConfigDMS command options

Running the `ConfigDMS` utility with no command options starts the `ConfigDMS` utility in the default graphical user interface mode. This configuration utility prompts you for the necessary parameters to create databases and configure the SOA Domain Management Server and optional Tivoli Common Object Repository support. For more information about running `ConfigDMS`, see "Running the `ConfigDMS` utility in Graphical User Interface mode" on page 138.

The command options for the `ConfigDMS` utility are as follows:

–console

This option runs the `ConfigDMS` utility in command-line mode, if you prefer to use this utility instead of the Install Shield graphical user interface. This option cannot be specified together with the **–silent** option. For more information, see "Running the `ConfigDMS` utility in console mode" on page 163.

Examples:

```
ConfigDMS -console
```

–silent [*dir_path*/]*silent_file*

This option runs the `ConfigDMS` utility in silent mode. The *silent_file* file is a simple properties file that you create, containing the necessary parameters to create databases and configure the SOA Domain Management Server and optional Tivoli Common Object Repository support. If this file is not stored in the same directory path where you run the `ConfigDMS` utility (either the `ITM_Home\CNPS\Products\KD4\latest\bin` directory or the `ITM_Home\CNPS\Products\KD4\bin` directory), specify the fully qualified directory path where this file is located.

For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.This option cannot be specified together with the **–console** option. For more information, see "Running the `ConfigDMS` utility in silent mode" on page 164. Examples:

```
ConfigDMS -silent dmsconfig_silent.txt
ConfigDMS -silent C:\Configurations\configdms.silent
```

–debug [*dir_path*/]*debug_file*

This option can be specified alone, or after specifying either the **–console** or **–silent** options. The `ConfigDMS` utility is run in either graphical user interface mode, console mode, or silent mode, and log information is written to the *debug_file* file for later examination and diagnosis of problems by IBM Software Support.

The debug log file is a plain text file stored in a specified directory path, or, if no directory path is specified, in the same directory where you run the `ConfigDMS` utility (either *`ITM_Home`*`\CNPS\Products\KD4\latest\bin` or *`ITM_Home`*`\CNPS\Products\KD4\bin`).

If you do not specify a file name for *debug_file*, the utility is not started, and you are presented with the syntax information as a reminder. Examples:

```
ConfigDMS -debug configdms_log.txt
ConfigDMS -silent C:\Properties\config.props -debug C:\KD4\logs\cnfgdms.log
```

-remoteSDMS

This option can be specified alone or together with the `-remoteTCORE` option. The `-remoteSDMS` option can be specified after the `–debug` option, or after specifying either the `–console` or `–silent` options. The `-remoteSDMS` option prevents the SQL migrate scripts for the SOA Domain Management Server from running locally. The `-remoteSDMS` option must be specified when upgrading or updating a remote SOA Domain Management Server database.

-remoteTCORE

This option can be specified alone or together with the `-remoteSDMS` option. The `-remoteTCORE` option can be specified after the `–debug` option, or after specifying either the `–console` or `–silent` options. The `-remoteTCORE` option prevents the SQL migrate scripts for Tivoli Common Object Repository from running locally. The `-remoteTCORE` option must be specified when upgrading or updating a remote Tivoli Common Object Repository database.

Logging information

Logging information is written to a log file in the *`ITM_Home`*`\logs` directory, named in this format: kd4_sdms_config*date_timestamp*.log. Scroll to the end of this log file for the most recent information. See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with problems you might encounter while configuring support for SOA Domain Management Server and Tivoli Common Object Repository.

If errors are encountered during configuration, messages are displayed with information to assist you in determining the problem. For information about the usual errors you might encounter and for a more complete description of error messages and recovery options, see *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*.

Running the `ConfigDMS` utility in Graphical User Interface mode

Running the `ConfigDMS` utility without specifying either the `–console` or `–silent` options starts the `ConfigDMS` with the InstallShield wizard graphical user interface.

Running the `ConfigDMS` utility from an ITCAM for SOA V7.2 installation

After you select the preferred language, a welcome page is presented with some brief information about the `ConfigDMS` utility. After you click **Next**, the `ConfigDMS` utility detects one of the following conditions:

SOA Domain Management Server or Tivoli Common Object Repository support is configured for ITCAM for SOA V7.2

In this case, the utility informs you that the application will be upgraded to the current version. See "Upgrading a version 7.1.1 topology configured locally" on page 202 for the procedure.

Important: If you are upgrading a database from version 7.1.1 (all versions) and the database is located remotely, you must use the *-remoteSDMS* or *-remoteTCORE* arguments to launch the `ConfigDMS` utility.

ITCAM for SOA support for SOA Domain Management Server and Tivoli Common Object Repository is not yet configured

In this case, the utility offers you choices to configure SOA Domain Management Server and, optionally, Tivoli Common Object Repository at the version 7.2 level. See "Configuring topology support for the first time" on page 208 for the procedure.

ITCAM for SOA V7.2 support for the SOA Domain Management Server is configured but not for Tivoli Common Object Repository

The utility offers you one or more of the following configuration choices:

- If your SOA Domain Management Server database password has changed recently, you can update the authentication in your current SOA Domain Management Server configuration. For the procedure, see "Updating authentication for SOA Domain Management Server" on page 217.
- You can configure the optional support for Tivoli Common Object Repository. For the procedure, see "Configuring the Tivoli Common Object Repository" on page 213.

ITCAM for SOA V7.2 support for the SOA Domain Management Server and Tivoli Common Object Repository are both configured

In this case, the utility offers you the following configuration choices:

- If your SOA Domain Management Server database password has changed recently, you can update the authentication in your current SOA Domain Management Server configuration. For the procedure, see "Updating authentication for SOA Domain Management Server" on page 217.
- If your Tivoli Common Object Repository database password has changed recently, you can update the authentication in your current Tivoli Common Object Repository configuration. For the procedure, see "Updating authentication for Tivoli Common Object Repository" on page 218.

Running the `ConfigDMS` utility from an ITCAM for SOA V7.2 Fix Pack 1 installation

After you select the preferred language, a welcome page is presented with some brief information about the `ConfigDMS` utility. After you click **Next**, the `ConfigDMS` utility detects one of the following conditions:

SOA Domain Management Server or Tivoli Common Object Repository support is configured for ITCAM for SOA V7.2 Fix Pack 1

In this case, the utility informs you that the application will be updated to the current version. See “Updating a version 7.2 topology configured locally” on page 142 for the procedure.

Important: If you are updating a database from version 7.2 and the database is located remotely, you must use the *-remoteSDMS* or *-remoteTCORE* arguments to start the `ConfigDMS` utility.

ITCAM for SOA support for SOA Domain Management Server and Tivoli Common Object Repository is not yet configured

In this case, the utility offers you choices to configure SOA Domain Management Server and, optionally, Tivoli Common Object Repository at the version 7.2 Fix Pack 1 level. See “Configuring topology support for the first time” on page 208 for the procedure.

ITCAM for SOA V7.2 Fix Pack 1 support for the SOA Domain Management Server is configured but not for Tivoli Common Object Repository

The utility offers you one or more of the following configuration choices:

- If your SOA Domain Management Server database password has changed recently, you can update the authentication in your current SOA Domain Management Server configuration. For the procedure, see “Updating authentication for SOA Domain Management Server” on page 217.
- You can configure the optional support for Tivoli Common Object Repository. For the procedure, see “Configuring the Tivoli Common Object Repository” on page 213.

ITCAM for SOA V7.2 Fix Pack 1 support for the SOA Domain Management Server and Tivoli Common Object Repository are both configured

In this case, the utility offers you the following configuration choices:

- If your SOA Domain Management Server database password has changed recently, you can update the authentication in your current SOA Domain Management Server configuration. For the procedure, see “Updating authentication for SOA Domain Management Server” on page 217.
- If your Tivoli Common Object Repository database password has changed recently, you can update the authentication in your current Tivoli Common Object Repository configuration. For the procedure, see “Updating authentication for Tivoli Common Object Repository” on page 218.

Upgrading topology support using the ConfigDMS utility

You can upgrade topology support from ITCAM for SOA version 7.1.1 to version 7.2. When you have configured topology support for ITCAM for SOA version 7.2, you must update topology to ITCAM for SOA version 7.2 Fix Pack 1.

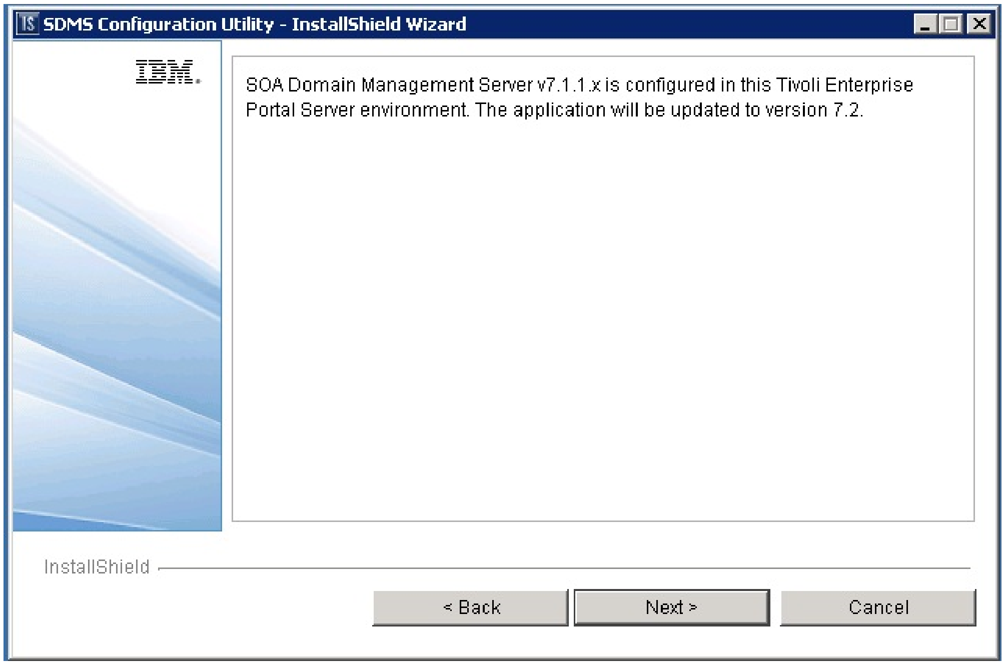
Upgrading a version 7.1.1 topology configured locally: If you have a configuration of SOA Domain Management Server and Tivoli Common Object Repository support from a previous version of ITCAM for SOA in your local Tivoli Enterprise Portal Server environment, the `ConfigDMS` utility upgrades this support to ITCAM for SOA version 7.2. When upgrading from ITCAM for SOA version 7.1.1 (all releases) to version 7.2, the utility does not prompt you for upgrade information.

Important:

- The process might take some time to complete as the database is upgraded, depending on its size. It can take 15 minutes or longer. Do not stop the `ConfigDMS` utility in the middle of an upgrade.
- If your SOA Domain Management Server database was created with Microsoft SQL Server 2000 in version 7.1.1, your database administrator must manually migrate the Microsoft SQL Server database to a supported database version (Microsoft SQL Server 2005 or Microsoft SQL Server 2008) before running the `ConfigDMS` utility.

To upgrade a topology, complete the following steps:

1. Start the ConfigDMS utility in graphical user interface mode. For more information, see "Running the `ConfigDMS` utility in Graphical User Interface mode" on page 138.
2. The utility informs you that the application will be updated to the current version.



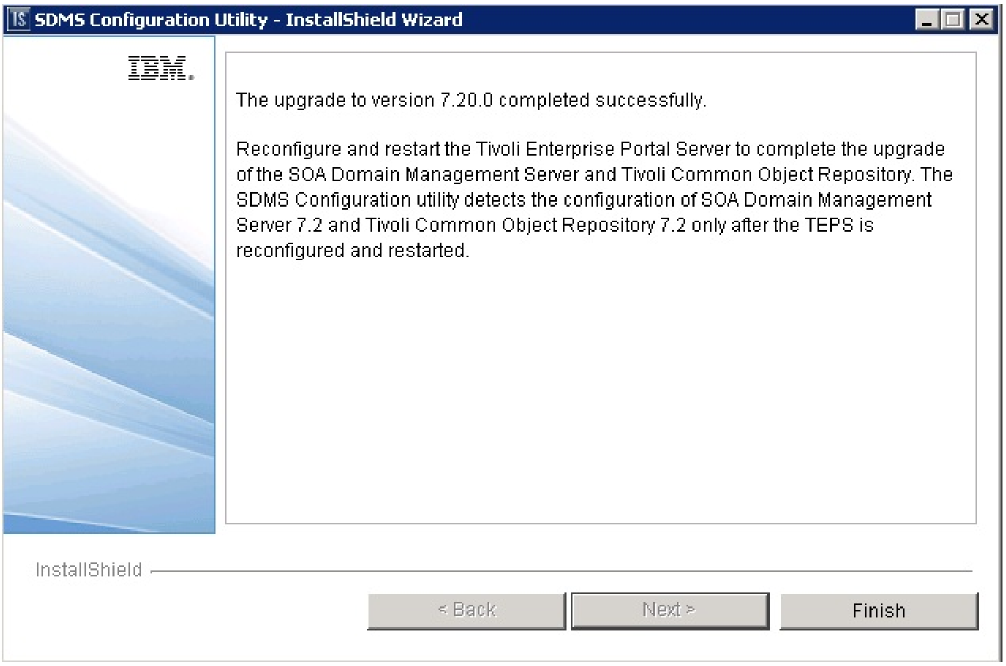
SDMS Configuration Utility - InstallShield Wizard

SOA Domain Management Server v7.1.1.x is configured in this Tivoli Enterprise Portal Server environment. The application will be updated to version 7.2.

Figure 18. Message indicating that the application will be updated to the current version

   Click **Next**.

3. The utility upgrades Tivoli Common Object Repository support to the current version. If there are errors, you are notified and the only option is to exit the utility. If you experience errors while upgrading your SOA Domain Management Server or Tivoli Common Object Repository support, consult with your local database administrator for assistance or contact IBM Software Support.
4. The utility notifies you that the upgrade has completed.



The upgrade to version 7.20.0 completed successfully.

Reconfigure and restart the Tivoli Enterprise Portal Server to complete the upgrade of the SOA Domain Management Server and Tivoli Common Object Repository. The SDMS Configuration utility detects the configuration of SOA Domain Management Server 7.2 and Tivoli Common Object Repository 7.2 only after the TEPS is reconfigured and restarted.

Figure 19. Message indicating that the upgrade is complete

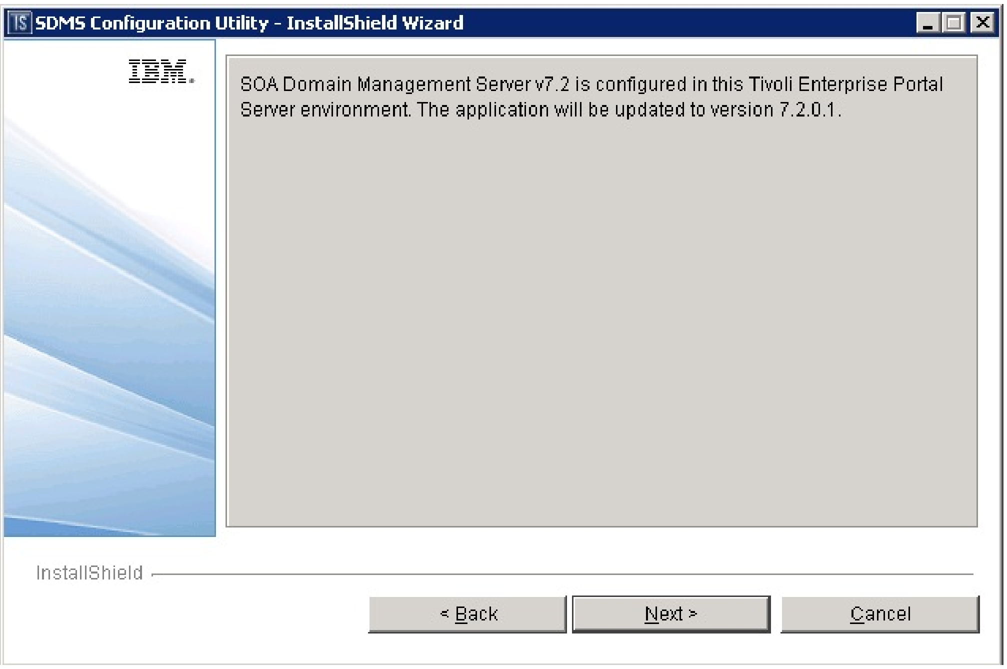
5. Click **Finish** to exit the utility.
6. Reconfigure and restart Tivoli Enterprise Portal Server for the upgrade to take effect. For more information about reconfiguring the portal server, see “Reconfiguring and restarting the Tivoli Enterprise Portal Server” on page 173.

The `collation.properties` and `bulkload.properties` files in the *ITM_Home*`\CNPS\Products\KD4\tcore\etc` directory are renamed to `bulkload.properties.backup` and `collation.properties.backup1`. (For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.) If you modified any properties in a previous version of these files, you must manually merge the changes into ITCAM for SOA version 7.2 files after migration is complete.

Updating a version 7.2 topology configured locally: If you already have a configuration of SOA Domain Management Server and Tivoli Common Object Repository support from a previous version of ITCAM for SOA in your local Tivoli Enterprise Portal Server environment, the `ConfigDMS` utility updates this support to ITCAM for SOA version 7.2 Fix Pack 1. When updating from ITCAM for SOA version 7.2 o version 7.2 Fix Pack 1, the utility does not prompt you for upgrade information.

To update a topology, complete the following steps:

1. Start the ConfigDMS utility in graphical user interface mode. For more information, see “Running the `ConfigDMS` utility in Graphical User Interface mode” on page 138.
2. The utility informs you that the application will be updated to the current version.

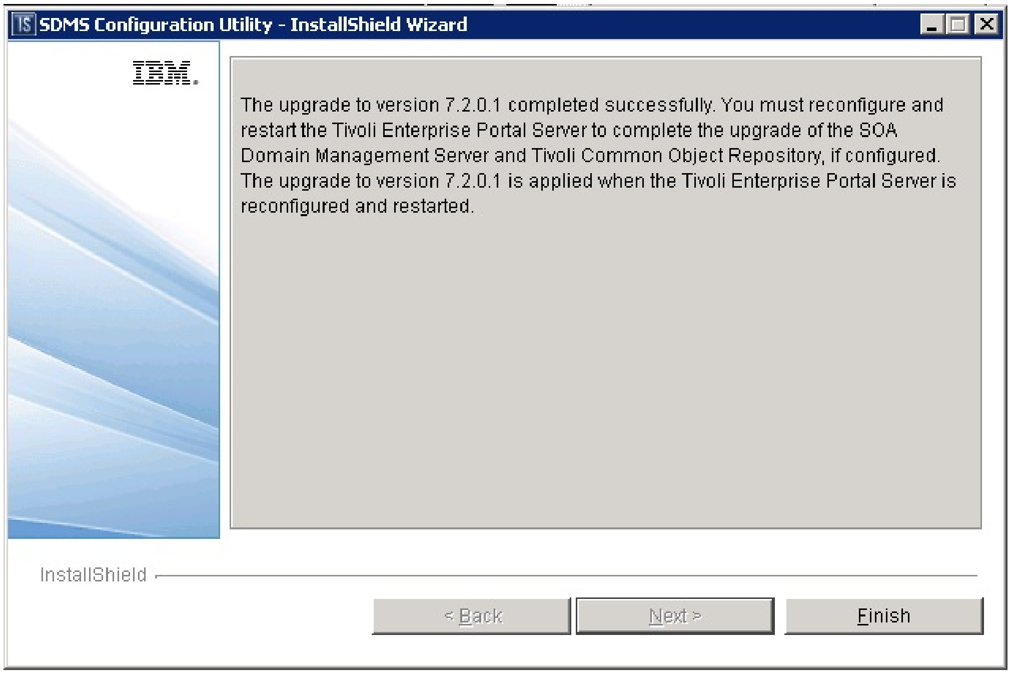


SOA Domain Management Server v7.2 is configured in this Tivoli Enterprise Portal Server environment. The application will be updated to version 7.2.0.1.

Figure 20. Message indicating that the application will be updated to the current version

Click **Next**.

3. The utility updates Tivoli Common Object Repository support to the version 7.2 Fix Pack 1. If there are errors, you are notified and the only option is to exit the utility. If you experience errors while upgrading your SOA Domain Management Server or Tivoli Common Object Repository support, consult with your local database administrator for assistance or contact IBM Software Support.
4. The utility notifies you that the update to version 7.2 Fix Pack 1 has completed.



The upgrade to version 7.2.0.1 completed successfully. You must reconfigure and restart the Tivoli Enterprise Portal Server to complete the upgrade of the SOA Domain Management Server and Tivoli Common Object Repository, if configured. The upgrade to version 7.2.0.1 is applied when the Tivoli Enterprise Portal Server is reconfigured and restarted.

Figure 21. Message indicating that the upgrade is complete

5. Click **Finish** to exit the utility.
6. Reconfigure and restart Tivoli Enterprise Portal Server for the upgrade to take effect. For more information about reconfiguring the portal server, see “Reconfiguring and restarting the Tivoli Enterprise Portal Server” on page 173.

The `collation.properties` and `bulkload.properties` files in the *ITM_Home*`\CNPS\Products\KD4\tcore\etc` directory are renamed to `bulkload.properties.backup` and `collation.properties.backup1`. (For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.) If you modified any properties in a previous version of these files, you must manually merge the changes into ITCAM for SOA version 7.2 Fix Pack 1 files after migration is complete.

Upgrading a previous topology configured remotely: If you already have a configuration of SOA Domain Management Server, or SOA Domain Management Server and Tivoli Common Object Repository from a previous version of ITCAM for SOA installed on a *remote* system, you must use the `ConfigDMS` utility to complete the following:

- Upgrade support for the databases to the later version of ITCAM for SOA:
  - If you are upgrading to ITCAM for SOA version 7.2 before you update to ITCAM for SOA version 7.2 Fix Pack 1, upgrade support for the databases to version 7.2.
  - If you are updating to ITCAM for SOA version 7.2 Fix Pack 1, update support for the databases to version 7.2 Fix Pack 1.
- Manually migrate the SOA Domain Management Server database schema on the remote system to the later version
- Reconfigure and restart the Tivoli Enterprise Portal Server.

To upgrade a remote DB2, Microsoft SQL Server, or Oracle database, complete the following steps:

1. If only the SOA Domain Management Server or the Tivoli Common Object Repository database is on a remote system, you must set the environment variable for the other local database.
2. On the Tivoli Enterprise Portal Server where the ITCAM for SOA agent is installed, run the `ConfigDMS` utility with the *-remoteSDMS* argument if the SOA Domain Management Server database is remote and the *-remoteTCORE* argument if the Tivoli Common Object Repository database is remote. For example:

   ```
   TEPS_home/Products/KD4/latest/bin/ConfigDMS.bat -remoteSDMS -remoteTCORE
   ```

   The *-remoteSDMS* and the *-remoteTCORE* arguments can be specified with either the *-console* or *-silent* arguments.

   If there are errors, you are notified and the only option is to exit the utility. If you experience errors while upgrading your SOA Domain Management Server or Tivoli Common Object Repository support, consult with your local database administrator for assistance or contact IBM Software Support. You are notified when the upgrade completes successfully, and can exit the utility
3. To migrate the SOA Domain Management Server database on a remote system, perform the following steps:
   a. Copy the `kd4RemoteDB.zip` file from *TEPS_home*`/Products/KD4/latest/bin/` to the remote database host.
   b. Verify that the databases and any required services are running on the remote host.
   c. If you are upgrading from ITCAM for SOA version 7.1.1 to version 7.2, locate the script to migrate the database schema from ITCAM for SOA version 7.1.1 on the remote system:
      - If the remote database is a DB2 database, run the following command as an administrator:

        ```
        kd4MigrateDB2db.bat sdms_db2_7113_to_72.sql DBNAME
        ```

        where *DBNAME* is the name of the SOA Domain Management Server database.
      - If the remote database is a Microsoft SQL Server database, run the following command as an administrator:

        ```
        kd4MigrateMSSQLdb.bat sdms_mssql_7113_to_72.sql DBNAME
        [sql-server-instance]
        ```

        Where:

        DBNAME
        The name of the SOA Domain Management Server database

        sql-server-instance
        The Microsoft SQL server instance name in the form of *database_hostname**instance-name*.

        database_hostname
        The name of the computer where the database server is installed.

        instance-name
        The instance name, for example, `localhost\MyInstance`. If no value is specified, the default instance is assumed.
      - If the remote database is an Oracle database, complete the following steps:

- Verify that the PATH system variable in your environment variables contains the Oracle bin directory where sqlplus.exe is located. For example, PATH=%PATH%;C:\app\Administrator\product\11.2.0\dbhome_1\bin.
- Set the ORACLE_SID environment variable to the name of the SOA Domain Management Server database. For example, ORACLE_SID=KD4SDMS.
- Run the following command as an Administrator:

  ```
  kd4MigrateOracledb.bat sdms_oracle_7113_to_72.sql
  DBNAME SDMS [DBUSER PASSWD]
  ```

  Where:

  DBNAME
  Name of the SOA Domain Management Server database. The name is the Oracle System Identifier of the database.

  DBUSER
  Name of the SOA Domain Management Server database user.

  PASSWD
  Password that is associated with *DBNAME*.

Important: The process might take some time to complete as the database is upgraded, depending on its size. It can take 15 minutes or longer. Do not stop the kd4MigrateDB2db.bat or the kd4MigrateOracledb.bat migrate script in the middle of an upgrade.

d. If you are updating from ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1, locate the script to migrate the database schema from ITCAM for SOA version 7.2 on the remote system.

- If the remote database is a DB2 database, run the following command as an administrator:

  ```
  kd4MigrateDB2db.bat sdms_db2_72_to_7201.sql DBNAME
  ```

  where *DBNAME* is the name of the SOA Domain Management Server database.
- If the remote database is a Microsoft SQL Server database, run the following command as an administrator:

  ```
  kd4MigrateMSSQLdb.bat sdms_mssql_72_to_7201.sql DBNAME
  [sql-server-instance]
  ```

  Where:

  DBNAME
  The name of the SOA Domain Management Server database

  sql-server-instance
  The Microsoft SQL server instance name in the form of *database_hostname\instance-name*.

  database_hostname
  The name of the computer where the database server is installed.

  instance-name
  The instance name, for example, localhost\MyInstance. If no value is specified, the default instance is assumed.
- If the remote database is an Oracle database, complete the following steps:

- Verify that the PATH system variable in your environment variables contains the Oracle bin directory where sqlplus.exe is located. For example, PATH=%PATH%;C:\app\Administrator\product\11.2.0\dbhome_1\bin.
- Set the ORACLE_SID environment variable to the name of the SOA Domain Management Server database. For example, ORACLE_SID=KD4SDMS.
- Run the following command as an Administrator:

  ```
  kd4MigrateOracledb.bat sdms_oracle_72_to_7201.sql
  DBNAME SDMS [DBUSER PASSWD]
  ```

  Where:

  DBNAME
  Name of the SOA Domain Management Server database. The name is the Oracle System Identifier of the database.

  DBUSER
  Name of the SOA Domain Management Server database user.

  PASSWD
  Password associated with *DBNAME*.

4. Reconfigure and restart Tivoli Enterprise Portal Server for the upgrade to take effect. For more information about reconfiguring the portal server, see "Reconfiguring and restarting the Tivoli Enterprise Portal Server" on page 173.

The collation.properties and bulkload.properties files in the *ITM_Home*\CNPS\Products\KD4\tcore\etc directory are renamed to bulkload.properties.backup and collation.properties.backup1. (For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.) If you modified any properties in a previous version of these files, you must manually merge the changes into the latest version of ITCAM for SOA after migration is complete.

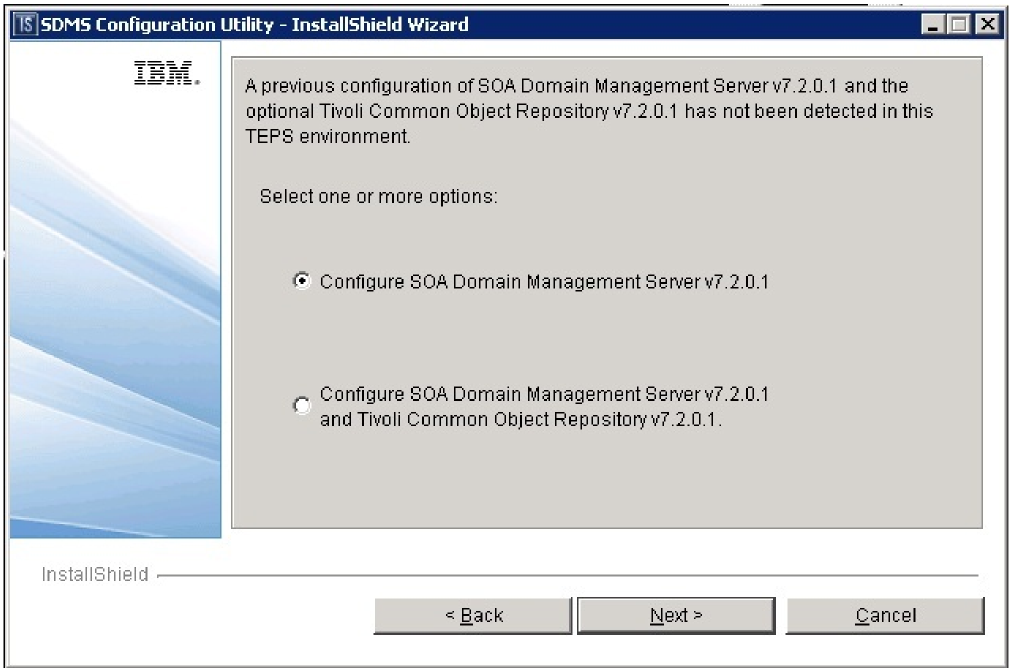
Configuring topology support using the ConfigDMS utility

If you do not have a previous installation of ITCAM for SOA, you can configure topology support for ITCAM for SOA version 7.2 Fix Pack 1 without first configuring topology support for ITCAM for SOA version 7.2.

Configuring topology support for the first time: If you do not have a previous configuration of SOA Domain Management Server topology support in your portal server environment, then the ConfigDMS utility configures this support for you.

You are asked to select one of the following options:

- Configure support for SOA Domain Management Server only.
- Configure support for both SOA Domain Management Server and Tivoli Common Object Repository.



A previous configuration of SOA Domain Management Server v7.2.0.1 and the optional Tivoli Common Object Repository v7.2.0.1 has not been detected in this TEPS environment.

Select one or more options:

● Configure SOA Domain Management Server v7.2.0.1

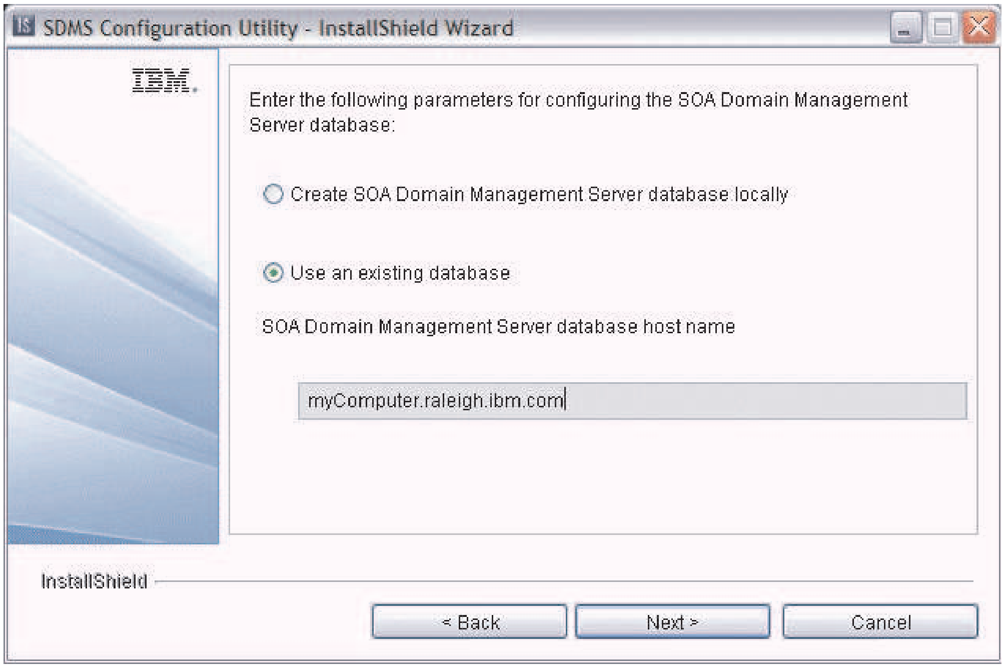
○ Configure SOA Domain Management Server v7.2.0.1 and Tivoli Common Object Repository v7.2.0.1.

Figure 22. Configuring topology support for the first time

For the procedures, see "Configuring the SOA Domain Management Server" and "Configuring the Tivoli Common Object Repository" on page 157.

Configuring the SOA Domain Management Server: To configure SOA Domain Management Server, complete the following steps:

1. Start the `ConfigDMS` utility in graphical user interface mode. For more information, see "Running the `ConfigDMS` utility in Graphical User Interface mode" on page 138.
2. Specify whether to create the SOA Domain Management Server database locally, or whether to use an existing (local or remote) database that you have previously created.



Enter the following parameters for configuring the SOA Domain Management Server database:

○ Create SOA Domain Management Server database locally

● Use an existing database

SOA Domain Management Server database host name

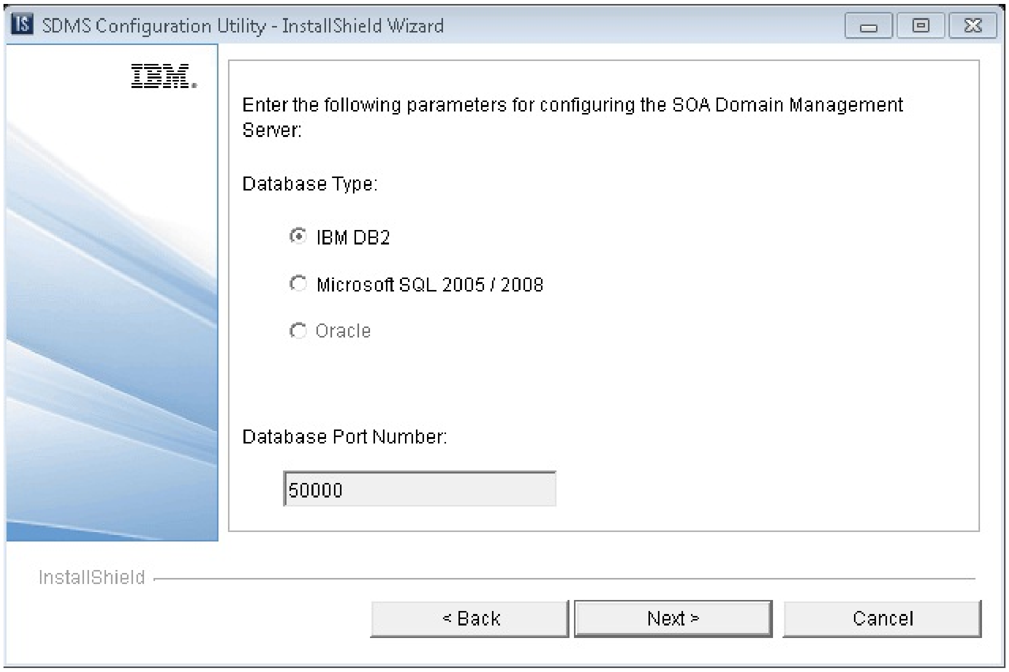
myComputer.raleigh.ibm.com

Figure 23. Options to create the SOA Domain Management Server database or use an existing database

If you prefer to use an existing local or remote database, select **Use an existing database** and enter the host name of the computer where the SOA Domain Management Server database is located. You can also specify *localhost* to use an existing local database.

Important: If you plan to use an Oracle database to support the SOA Domain Management Server, you must use an existing database that is either on the local portal server or is on a remote database server. You must also use an Oracle database for the Tivoli Common Object Repository. For information about using script files to manually create the local or remote SOA Domain Management Server database before running the `ConfigDMS` utility, see “Creating the SOA Domain Management Server database” on page 120.

3. Select the database type.



SDMS Configuration Utility - InstallShield Wizard

Enter the following parameters for configuring the SOA Domain Management Server:

Database Type:

● IBM DB2

○ Microsoft SQL 2005 / 2008

○ Oracle

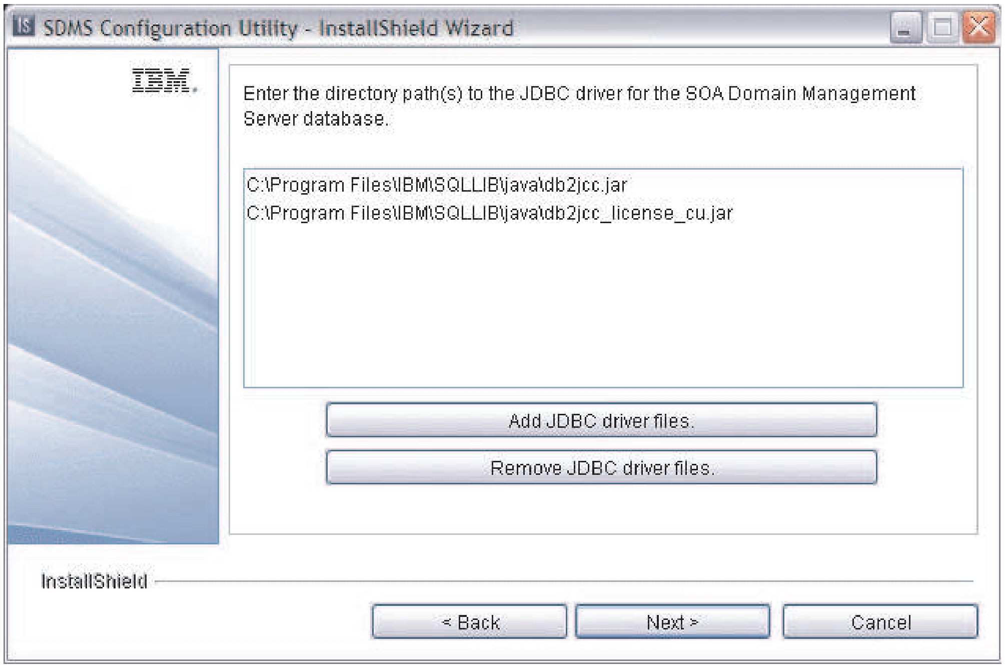
Database Port Number:

50000

Figure 24. Configuring the SOA Domain Management Server

The three possible database types are DB2, Microsoft SQL Server, and Oracle. This parameter is automatically obtained from the Tivoli Enterprise Portal Server configuration, and the default value for this parameter is set to the current database type.

4. If you selected DB2 as the database type, complete the following steps
   a. Enter the database port number. The default port number is `50000`.
   b. Specify the fully qualified directory path to the JDBC driver class files.



SDMS Configuration Utility - InstallShield Wizard

Enter the directory path(s) to the JDBC driver for the SOA Domain Management Server database.

```
C:\Program Files\IBM\SQLLIB\java\db2jcc.jar
C:\Program Files\IBM\SQLLIB\java\db2jcc_license_cu.jar
```

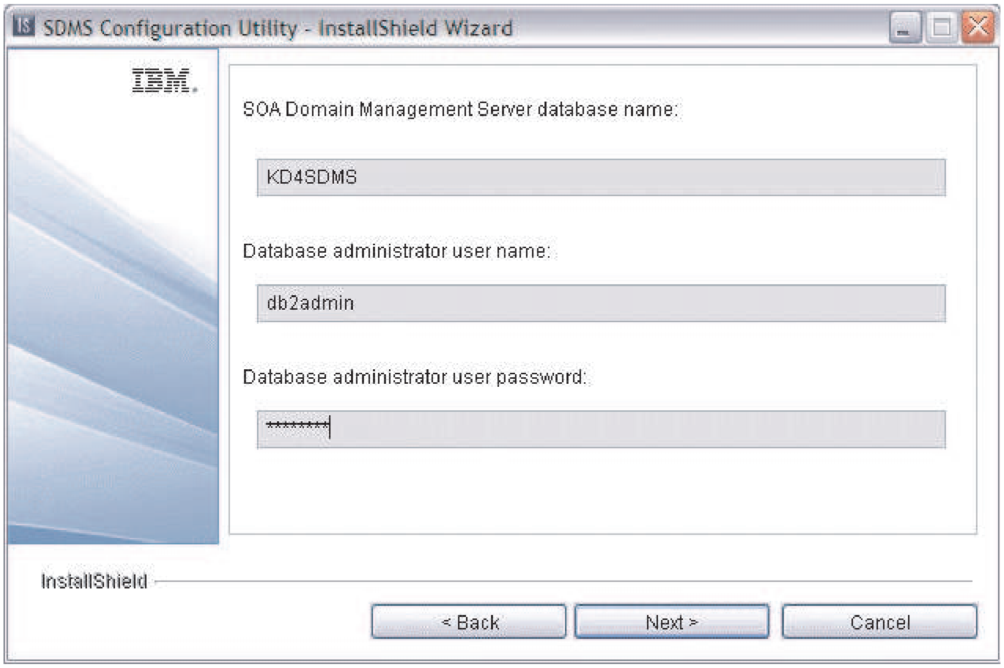
Figure 25. Specifying the JDBC drivers

The utility searches for the driver files based on where your database application is installed, and presents these files as defaults. You can accept these defaults or specify others as needed. The following files are the specific files that the utility searches for:

```
C:\Program Files\IBM\SQLLIB\java\db2jcc.jar
C:\Program Files\IBM\SQLLIB\java\db2jcc_license_cu.jar
```

These JDBC drivers, obtained from the database server, are needed on the computer where the portal server is installed (where SOA Domain Management Server support is being configured).

c. Enter the name of the SOA Domain Management Server database.



SDMS Configuration Utility - InstallShield Wizard

SOA Domain Management Server database name: KD4SDMS

Database administrator user name: db2admin

Database administrator user password: ********

Figure 26. Specifying the SOA Domain Management Server database name and database user

The default name is KD4SDMS and has a limit of 8 characters.

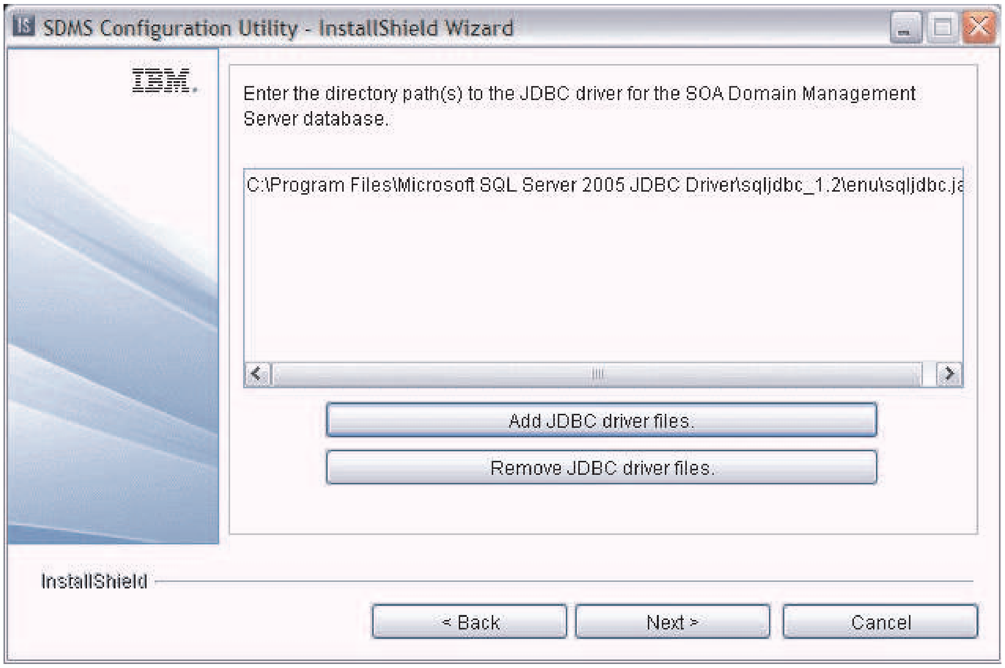
Remember: If you specified to create the SOA Domain Management Server database locally and this database name exists on the local system, it is dropped and recreated. If you want the configuration utility to create this database for you and you do not want to drop an existing database, specify a different name.

d. Enter the database administrative user name and password (for example, the default user name and password, *db2admin*). This user name must exist, and the configuration utility validates the specified password before continuing. For more information about authorization required for this database user, see "Database and User Permissions" on page 115.

5. If you selected Microsoft SQL Server as the database type, complete the following steps:

   a. Enter the database port number. For either Microsoft SQL Server 2005 or Microsoft SQL Server 2008, the default port number is *1433*.

   b. Enter the fully qualified directory path to the JDBC driver class files (`sqljdbc.jar`).


SDMS Configuration Utility - InstallShield Wizard

Enter the directory path(s) to the JDBC driver for the SOA Domain Management Server database.

C:\Program Files\Microsoft SQL Server 2005 JDBC Driver\sqljdbc_1.2\enu\sqljdbc.ja

Figure 27. Specifying the Microsoft SQL Server JDBC drivers

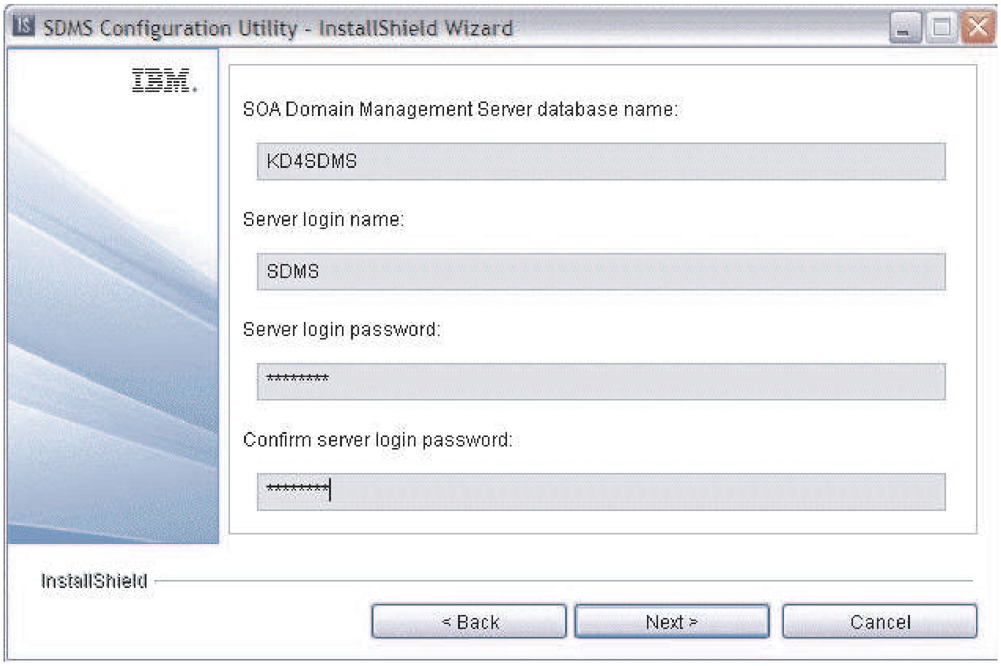
Only the Microsoft JDBC driver for Microsoft SQL Server is supported and is available as a free download from the Microsoft Developer Network http://www.microsoft.com/downloads.

6. Enter the name of the SOA Domain Management Server database to be created. The default name is *KD4SDMS* and has a limit of 128 characters.

   If you specify a new database server level login, the utility displays a message that notes that, with Microsoft SQL Server, a new database server level login is created if one does not exist.

   If you select the option to create the SOA Domain Management Server database locally and this database name exists on the local system, it is dropped and re-created. If you want the utility to create this database for you and you do not want to drop an existing database, specify a different name.

7. Enter the server login name and password.



SOA Domain Management Server database name: KD4SDMS

Server login name: SDMS

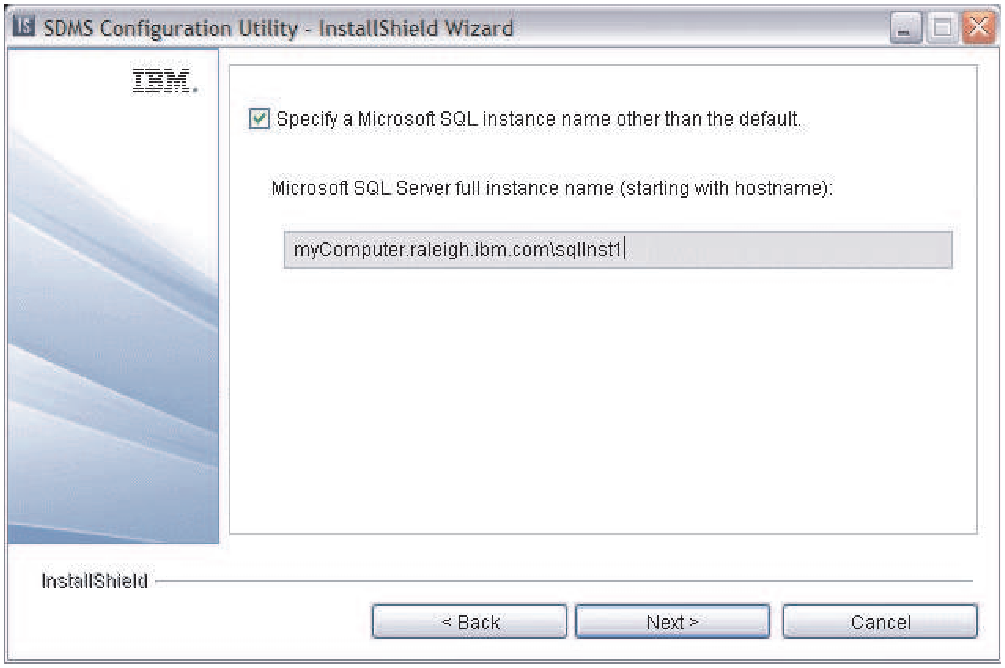
Server login password: *********

Confirm server login password: *********

Figure 28. Specifying the SOA Domain Management Server database name and server login access

You can specify any login name except the reserved name, *sa*. If the server login name exists, the configuration utility validates the password before continuing, but if the server login name does not exist, the configuration utility creates a server level login for the specified name in the Microsoft SQL Server registry and assigns it the password that you specify. If you ran the `kd4MakeMSSQLdb` script to manually create the database, then specify the server login name and password that were passed to that script.

8. Enter the Microsoft SQL Server instance name.


SDMS Configuration Utility - InstallShield Wizard

☑ Specify a Microsoft SQL instance name other than the default.

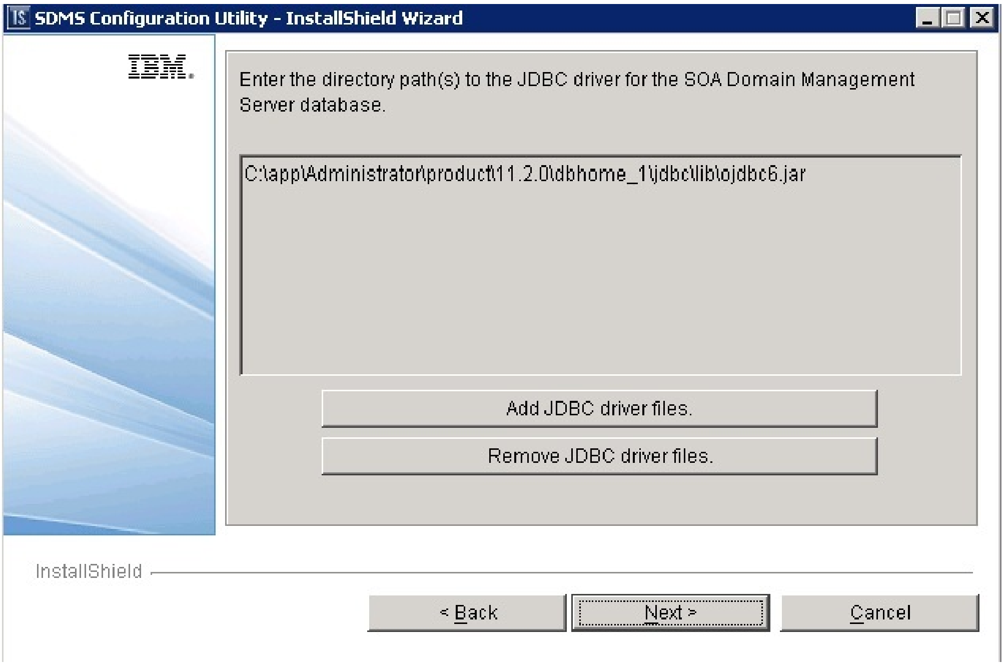
Microsoft SQL Server full instance name (starting with hostname):

myComputer.raleigh.ibm.com\sqlInst1

Figure 29. Specifying the Microsoft SQL Server instance name other than the default value

To use a named instance instead of the default instance, select the check box and enter the preferred instance name in the provided field. The full instance name consists of the host name and instance name separated by a backslash character (\), similar to the example shown in Figure 29. The host name must match the short host name (that is, the portion of the host name without the domain designation) of your Microsoft SQL Server.

9. If you selected Oracle as the database type, complete the following steps:
   a. Enter the fully qualified host name of the Oracle database server.
   b. Enter the database port number. The default port number is `1521`.
   c. Enter the fully qualified directory path to the Oracle JDBC driver. You must specify the fully qualified directory path to the `ojdbc6.jar` driver. For example:`C:\Program Files\oracle-jdbc-driver\ojdbc6.jar`



SDMS Configuration Utility - InstallShield Wizard

Enter the directory path(s) to the JDBC driver for the SOA Domain Management Server database.

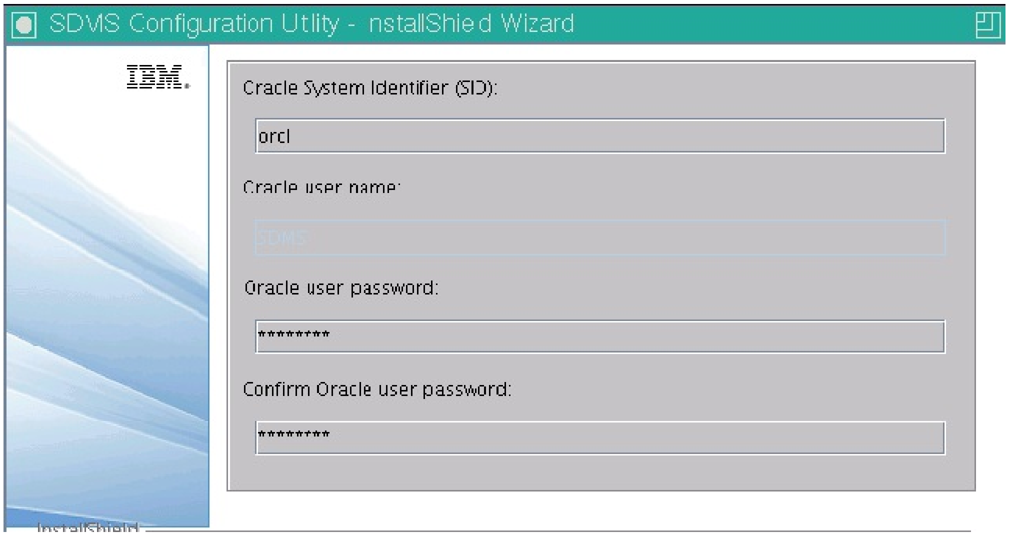
C:\app\Administrator\product\11.2.0\dbhome_1\jdbc\lib\ojdbc6.jar

Figure 30. Specifying the path to the Oracle JDBC driver

Restriction: The `ojdbc6.jar` JDBC driver must be used with Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2. For more information about this restriction, see technote.
If you installed Oracle 10g Release 2, you must download the `ojdbc6.jar` driver from the Oracle website because it is not provided with Oracle 10g Release 2.

d. Enter the Oracle system identifier. Set the Oracle system identifier to the system identifier specified when you ran the `KD4InitOracleDB` script.

e. Enter the he Oracle user password. Set it to the user password specified when you ran the `kd4InitOracleDb` script.



SDVIS Configuration Utlity - nstallShied Wizard

Cracle System Identifier (SID): orcl

Cracle user name: SDMS

Oracle user password: *********

Confirm Oracle user password: *********

Figure 31. Specifying the Oracle System identifier, user name and password

f. The utility validates the specified user name and password and attempts to configure the SOA Domain Management Server. If there are errors, you are notified and can go back and correct any specified parameters, or you can exit the configuration utility.

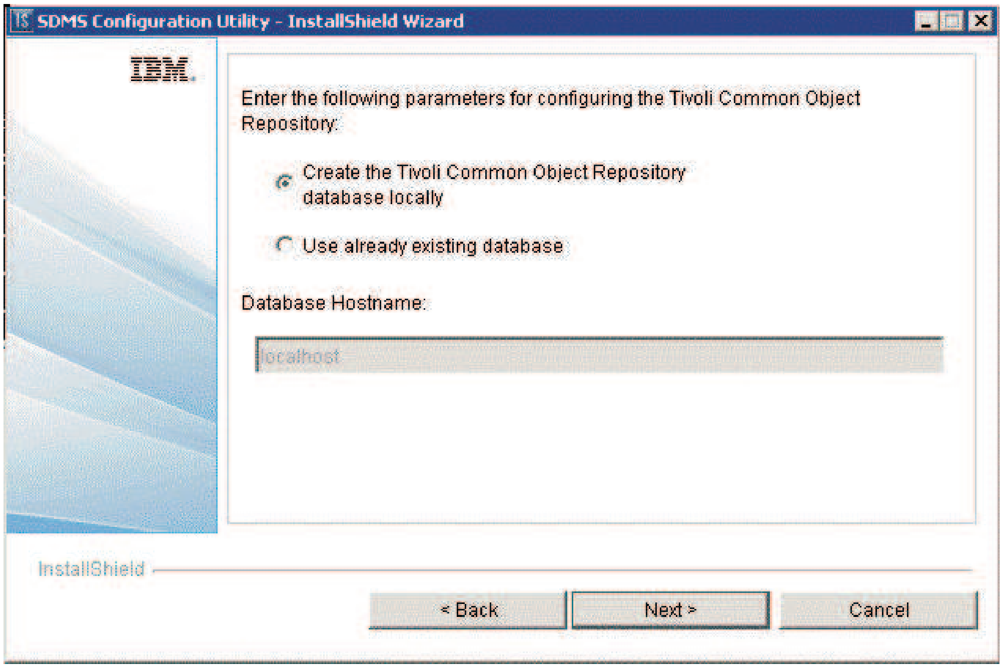
   When the configuration completes successfully, you are notified. If you selected to configure only the SOA Domain Management Server, you can exit the configuration utility. If you selected to configure both SOA Domain Management Server and Tivoli Common Object Repository, click **Next** to continue that configuration. See "Configuring the Tivoli Common Object Repository."

10. If you are not configuring Tivoli Common Object Repository, exit the utility and reconfigure and restart the Tivoli Enterprise Portal Server for the configuration to take effect. For the procedure, see "Reconfiguring and restarting the Tivoli Enterprise Portal Server" on page 173. Reconfiguring Tivoli Enterprise Portal Server might take 5-10 minutes to complete. During this time the Manage Tivoli Enterprise Monitoring Services utility might appear to be inoperable.

For information about the additional steps that are required to verify the installation and to enable access to the ITCAM for SOA Navigator in the Tivoli Enterprise Portal, see Part 5, "Completing your installation," on page 495. Be sure to complete all of the installation and verification steps that are documented in this guide before using the product.

Configuring the Tivoli Common Object Repository: To configure SOA Domain Management Server, complete the following steps:

1. Start the `ConfigDMS` utility in graphical user interface mode, if it is not started. For more information, see "Running the `ConfigDMS` utility in Graphical User Interface mode" on page 138.
2. Specify whether to create the Tivoli Common Object Repository database locally, or whether to use an existing (local or remote) database that you have previously created.



SDMS Configuration Utility - InstallShield Wizard

Enter the following parameters for configuring the Tivoli Common Object Repository:

● Create the Tivoli Common Object Repository database locally

○ Use already existing database

Database Hostname:

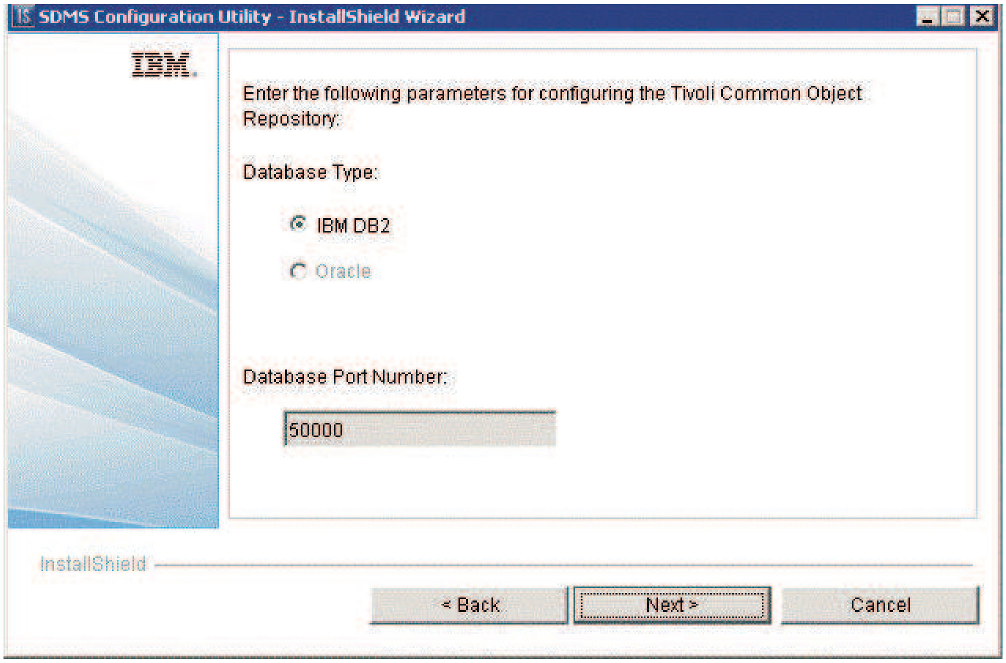
localhost

Figure 32. Configuring the Tivoli Common Object Repository

If you prefer to use an existing local or remote database, select **Use an existing database** and enter the host name of the computer where the Tivoli Common Object Repository database is located. You can also specify *localhost* to use an existing local database.

Important: If you plan to use an Oracle database to support the Tivoli Common Object Repository, you must use an existing database that is either on the local portal server or is on a remote database server. You must also use an Oracle database for the SOA Domain Management Server.
If you are configuring a remote Tivoli Common Object Repository database that you previously created (for example, with the `make_db2_db.bat` script for a DB2 database), specify the fully qualified host name for the computer where the remote database server is located.

3. Select the database type.


SDMS Configuration Utility - InstallShield Wizard

Enter the following parameters for configuring the Tivoli Common Object Repository:

Database Type:

● IBM DB2

○ Oracle

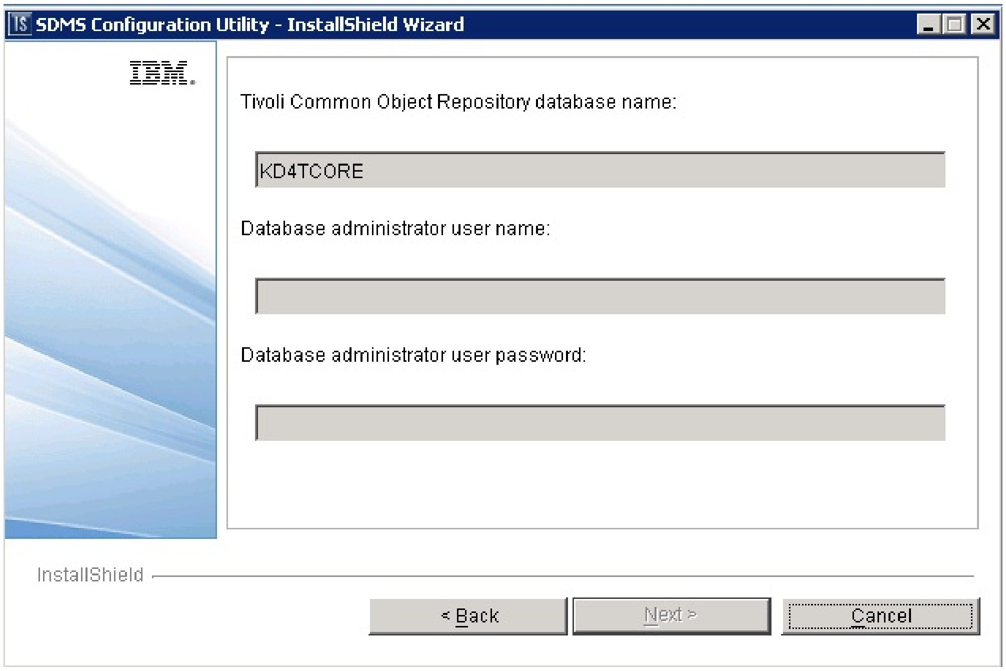
Database Port Number:

50000

Figure 33. Configuring the Tivoli Common Object Repository

If you are creating a database with the ConfigDMS utility, the option IBM DB2 is available for selection, and the option Oracle is unavailable. If you selected the option to use an existing database, both options are available for selection.

4. If you selected DB2 as the database type, complete the following steps:
   a. Enter the database port number. The default port number is 50000.
   b. Enter name of the Tivoli Common Object Repository database. The default name is KD4TCORE and has a limit of 8 characters.



Tivoli Common Object Repository database name:

KD4TCORE

Database administrator user name:

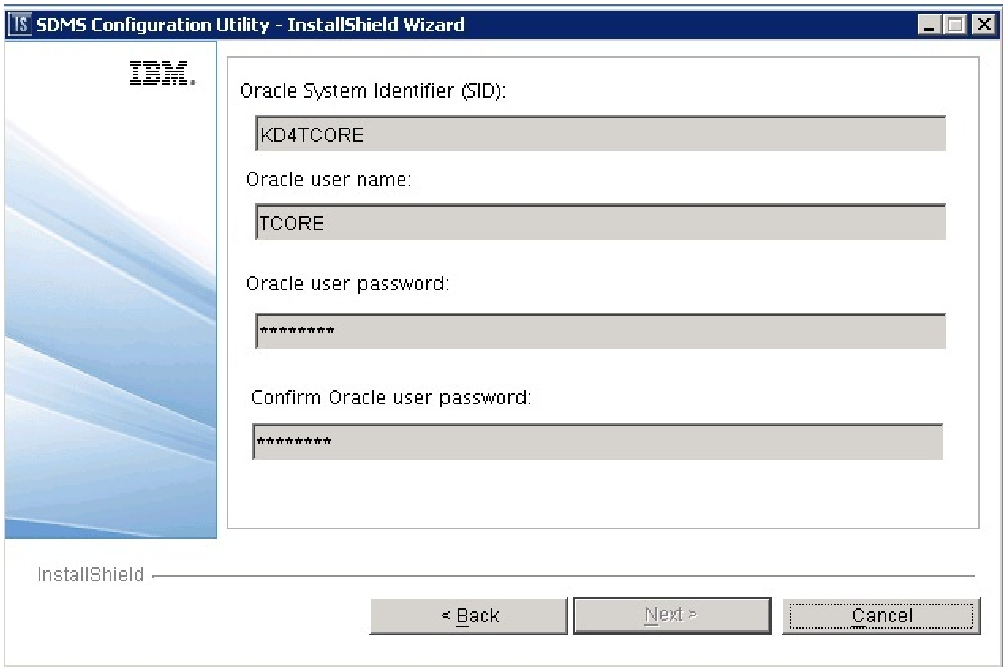
Database administrator user password:

Figure 34. Specifying the Tivoli Common Object Repository database name and database user

If you create the Tivoli Common Object Repository database locally and this database name exists on the local system, it is dropped and recreated. If you want the configuration utility to create this database for you and you do not want to drop an existing database, specify a different name. Likewise, if you use the `ConfigDMS` utility to create a local database for the SOA Domain Management Server and a local database for the Tivoli Common Object Repository, you must specify different names for each database.

c. Enter the database administrative user name and password (for example, the default user name and password, *db2admin*). This user name must exist, and the configuration utility validates the specified password before continuing. For more information about authorization required for this database user, see "Database and User Permissions" on page 115.

5. If you selected Oracle as the database type, complete the following steps:
   a. Enter the fully qualified host name of the Oracle database server.
   b. Enter the database port number. The default port number is *1521*.
   c. Enter the Oracle system identifier. Set the Oracle system identifier to the system identifier specified when you ran the `make_ora_user.bat` script.



Oracle System Identifier (SID):

KD4TCORE

Oracle user name:

TCORE

Oracle user password:

****

Confirm Oracle user password:

****

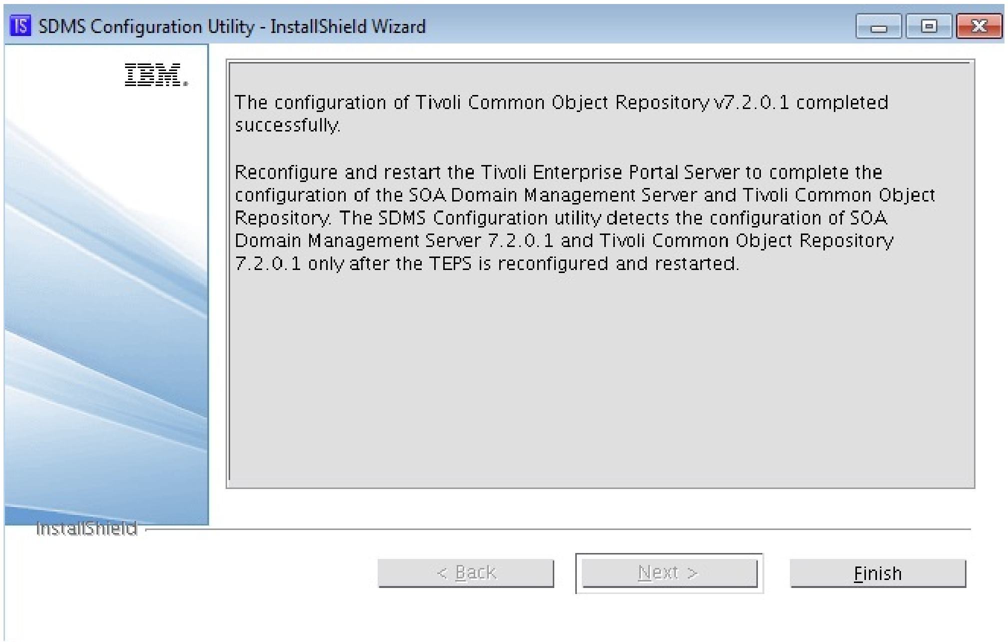
Figure 35. Specifying the Tivoli Common Object Repository Oracle System Identifier

d. Enter the Oracle user name. Specify the Oracle user that was entered when you ran the `make_ora_user.bat` script.

e. Enter the Oracle user password. Set the Oracle user password to the user password specified when you ran the `make_ora_user.bat` script.

f. The utility validates the specified user name and password.

6. The utility configures Tivoli Common Object Repository. If there are errors, you are notified and you can go back and correct any specified parameters, or you can exit the utility.
7. The utility informs you that the configuration is complete:



The configuration of Tivoli Common Object Repository v7.2.0.1 completed successfully.

Reconfigure and restart the Tivoli Enterprise Portal Server to complete the configuration of the SOA Domain Management Server and Tivoli Common Object Repository. The SDMS Configuration utility detects the configuration of SOA Domain Management Server 7.2.0.1 and Tivoli Common Object Repository 7.2.0.1 only after the TEPS is reconfigured and restarted.

Figure 36. Recommendation to reconfigure and restart Tivoli Enterprise Portal Server

8. Click **Finish** to exit the utility.
9. Reconfigure and restart Tivoli Enterprise Portal Server for the configuration to take effect. For the procedure, see "Reconfiguring and restarting the Tivoli Enterprise Portal Server" on page 173. Reconfiguring Tivoli Enterprise Portal Server might take 5-10 minutes to complete. During this time the Manage Tivoli Enterprise Monitoring Services utility might appear to be inoperable.

For information about the additional steps that are required to verify the installation and to enable access to the ITCAM for SOA Navigator in the Tivoli Enterprise Portal, see Part 5, "Completing your installation," on page 495. Be sure to complete all of the installation and verification steps that are documented in this guide before using the product.

Updating authentication using the ConfigDMS utility

You can update the SOA Domain Management Server authentication if the DB2 or Oracle password is changed in your database application.

Updating authentication for SOA Domain Management Server: You can update the SOA Domain Management Server authentication if the DB2, Microsoft SQL Server, or Oracle password is changed in your database application.

Updating authentication for a DB2, Microsoft SQL Server, or Oracle database

To update the SOA Domain Management Server authentication for a DB2, Microsoft SQL Server, or Oracle database, complete these steps:

1. Stop the Tivoli Enterprise Portal Server.
2. Open a command prompt window.
3. Run the SOA Domain Management Server Configuration utility from the `ITM_HOME\CNPS\Products\KD4\bin` directory.

   For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
4. Select **Update SOA Domain Management Server Authentication**.

5. Specify the new value in the field provided.

   The configuration utility verifies the new password by connecting to the database, and you are notified of any errors. You can return to the previous configuration utility page to correct your input before trying again.
6. Exit the utility.
7. Start the Tivoli Enterprise Portal Server.

You do not have to reconfigure Tivoli Enterprise Portal Server after updating the authentication, but you must restart the Tivoli Enterprise Portal Server for the authentication update to take effect.

Updating authentication for Tivoli Common Object Repository: You can update the Tivoli Common Object Repository authentication if the DB2 or Oracle password is changed in your database application.

Important: This action does not change the password, it updates the Tivoli Common Object Repository configuration with the new password information only. You must still use the database application to actually change and manage your database user passwords.

Updating authentication for a DB2 or Oracle database

To update the Tivoli Common Object Repository authentication for a DB2 or Oracle database, complete these steps:
1. Stop the Tivoli Enterprise Portal Server.
2. Open a command prompt window.
3. Run the SOA Domain Management Server Configuration utility from the directory `*ITM_HOME*\CNPS\Products\KD4\bin`.
4. Select the radio button to **Update Tivoli Common Object Repository Authentication**.
5. Specify the new value in the field provided.

   The configuration utility verifies the new password by connecting to the database, and you are notified of any errors. You can return to the previous configuration utility page to correct your input before trying again.
6. Exit the utility.
7. Start the Tivoli Enterprise Portal Server.

   You do not have to reconfigure Tivoli Enterprise Portal Server after updating the authentication, but you must restart the Tivoli Enterprise Portal Server for the authentication update to take effect.

Running the `ConfigDMS` utility in console mode

Running the `ConfigDMS` utility with the `–console` option starts the `ConfigDMS` utility in the command line.

You are prompted to select a language, and then a welcome response is displayed in the command line processor window, and you are prompted to continue by typing a numerical response:
- Type `1` to continue.
- Type `3` to cancel the wizard.
- Type `5` to display the response message and your choices again.

Throughout the use of the wizard in console mode, you must respond by typing one of several valid responses. The wizard presents the same basic selection options as described in "Running the ConfigDMS utility in Graphical User Interface mode" on page 138.

After exiting the utility, if you only updated authentication, you must restart Tivoli Enterprise Portal Server for the update to take effect. If you configured or upgraded support for SOA Domain Management Server or Tivoli Common Object Repository, you must rebuild and restart the Tivoli Enterprise Portal Server configuration for the configuration to take effect. For the procedure, see "Reconfiguring and restarting the Tivoli Enterprise Portal Server" on page 173.

Changing the character set code page

In some situations, you might find that some characters on the ConfigDMS utility pages are not displayed correctly, possibly substituted with question mark (?) or other unexpected characters. This might occur if, for example, you are running on a Windows operating system in Japanese and you choose to run the ConfigDMS utility in German.

To resolve this problem in console mode, you can change the Microsoft Windows character set code page for the current command prompt, with the **CHCP** command before running the ConfigDMS utility:

- For Italian, French, Spanish, and German languages, run this command:
  ```
  chcp 1252
  ```
- For Brazilian Portuguese, run this command:
  ```
  chcp 850
  ```

After running the CHCP command, run the ConfigDMS utility again in console mode and select a language. If the problem persists, you might have to change the font that is displayed by the console.

Important: The workaround is only required if you are running the ConfigDMS utility or the ConfigDC utility in console mode and some characters are not displayed correctly.

Running the ConfigDMS utility in silent mode

Running the ConfigDMS utility with the −silent [*dir_path*\]*silent_file* option starts the ConfigDMS utility in silent mode, using properties defined in the *silent_file* properties file.

Restriction: You cannot use the −silent mode and −console mode together.

When you run the ConfigDMS utility in silent mode, the configuration parameters are read from a simple text properties file, *silent_file*, that you create in advance. A typical properties file might look similar to the following example:

```
# Sample silent configuration file - silent file to deploy SDMS and TCORE
# File version - make sure that you are using proper version of silent file.
version=7.20.01.00

config_sdms=yes
config_tcore=no
update_sdms_auth=no
update_tcore_auth=no
update_sdms=no
update_tcore=no
upgrade=no
```

```
# SDMS section
# Supported values on Windows are "db2", "mssql2005" and "oracle"
# NOTE: For MS SQL 2008 use the value "mssql2005"
sdms_db_type=db2

# Use default port - uncomment the property to set to a different value
#sdms_db_port=
# Sample JDBC path when SDMS is configured to use DB2
sdms_jdbc_path=C\:\\Program Files\\IBM\\SQLLIB\\java\\db2jcc.jar;C\:\\
Program Files\\IBM\\SQLLIB\\java\\db2jcc_license_cu.jar

# Sample JDBC path when SDMS is configured to use MS SQL 2005 or 2008
# sdms_jdbc_path=C\:\\Program Files\\Microsoft SQL Server 2005
JDBC Driver\\sqljdbc_1.2\\enu\\sqljdbc.jar

# Sample JDBC path when SDMS is configured to use Oracle. The location of the
Oracle 10g Release 2 JDBC driver must be specified.
# sdms_jdbc_path=C\:\\oracle--jdbc-driver\\ojdbc6.jar

# Supported values are:
# 'yes' if SDMS database need to be created locally. 'yes' is not supported when
sdms_db_type is set to "oracle"
# 'no'  if SDMS is configured to use existing database
sdms_db_create_locally=yes

# When the database type is Oracle, this property specifies the
Oracle System Identifier (SID)sdms_db_name=KD4SDMS

# IMPORTANT: For MS SQL database the user ID sa is a reserved name that cannot
be used for logging in to the database server.
# IMPORTANT: For an Oracle database, this property is ignored and SDMS is used
as the Oracle database user name.
sdms_db_user=sdms
sdms_db_password=secret1

# Uncomment this property when SDMS is configured to use existing database
# on host different then 'localhost'
# sdms_db_host=localhost

# Uncomment this property when SDMS is configured to MS SQL 2005 or 2008 and
# instance other than default should be used. Instance name should be in form
hostname\instance_name
# sdms_mssql_instance=hostname\\sample_instance

# TCORE section
# Supported values on Windows are "db2" and "oracle"
# IMPORTANT:  When "oracle" is specified , the sdms_db_type property must
also be set to "oracle".tcore_db_type=db2

# Supported values are:
# 'yes' if TCORE database need to be created locally. 'yes' is not supported when
tcore_db_type is set to "oracle"
# 'no'  if TCORE is configured to use existing database
tcore_db_create_locally=yes

# Uncomment this property when TCORE is configured to use existing database
# on host different then 'localhost'
# tcore_db_host=localhost

# Use default port - uncomment the property to set to a different value
# tcore_db_port=
tcore_db_name=KD4TCORE
tcore_db_user=tcore
tcore_db_password=secret1
```

Remember: Make sure that you use the version of the file from ITCAM for SOA version 7.2 Fix Pack 1.

When you create a silent response properties file, keep in mind these considerations:

- A line in the file that starts with the # character is treated as a comment, and is not processed. If the # character is used elsewhere in the line, it is not considered to be the start of a comment. This means that you can use the # character in passwords or for other uses.
- The properties file is coded with the ISO 8859-1 character set.
- The properties file can include only one *version* property. For ITCAM for SOA version 7.2 Fix Pack 1, the only valid value of this property is the predefined value *07.20.01.00*.
- Each property is described on a separate line, in the following format: *Property = value*.

  Property
  The name of property. The list of valid properties that you can configure is shown in Table 20.

  Value The value of the property. Default values for some properties are already provided. You can erase default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can simply comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case-sensitive.
- Sample properties files (sample_silent_unix.cfg and sample_silent_win.cfg) are packaged with the SOA Domain Management Server Configuration utility. These files are available in `*ITM_Home*\CNPS\Products\KD4\latest\bin`, where *ITM_Home* is the location where Tivoli Monitoring is installed.

  For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.

Table 20. Available properties for running the SOA Domain Management Server Configuration utility in silent mode

Property	**Required (Yes/No)**	**Possible values**	**Upgrade of SDMS only**	**Upgrade of SDMS and TCORE**	**Comment**
version	Yes				Version number of the properties file, and must be set to the value of *7.20.01.00*.
config_sdms	No	*yes* or *no*			Specifies whether to configure SOA Domain Management Server. If this property is not specified, the default value of *No* is assumed.
config_tcore	No	*yes* or *no*			Specifies whether to configure the Tivoli Common Object Repository. If this property is not specified, the default value of *No* is assumed.

Table 20. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
update_sdms	No	*yes* or *no*			Specifies whether to update the configuration of SOA Domain Management Server to the latest version when a fix pack or interim fix is installed. If this property is not specified, the default value of *No* is assumed.
update_tcore	No	*yes* or *no*			Specifies whether to update the configuration of Tivoli Common Object Repository to the latest version when a fix pack or interim fix is installed. If this property is not specified, the default value of *No* is assumed.
update_sdms_auth	No	*yes* or *no*			Specifies whether to update the authentication for SOA Domain Management Server by changing the database password. If this property is not specified, the default value of *No* is assumed
update_tcore_auth	No	*yes* or *no*			Specifies whether to update the authentication for Tivoli Common Object Repository by changing the database password. If this property is not specified, the default value of *No* is assumed
upgrade	No	*yes* or *no*	X	X	Specifies whether to upgrade or update a previous configuration of SOA Domain Management Server and Tivoli Common Object Repository to version 7.2 or version 7.2 Fix Pack 1, depending on already configured components. If this property is not specified, the default value of *No* is assumed.
sdms_db_type	No	*db2* or *mssql2005*, or *oracle*			Specifies the type of database server that is used for the SOA Domain Management Server database. If this property is not specified, the value is obtained from the Tivoli Enterprise Portal Server configuration. For Microsoft SQL Server 2008, use the value mssql2005.The Microsoft SQL Server database type is supported only on Windows operating systems.

Table 20. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
sdms_db_port	Yes, when upgrading from SOA Domain Management Server version 7.1.1 to version 7.2 when SOA Domain Management Server is configured to use Microsoft SQL Server.		X (only if using MS SQL Server database)	X (only if using MS SQL Server database)	Specifies the port number for the DB2, Microsoft SQL Server, or Oracle database server where the SOA Domain Management Server database is created. If this property is not specified, the default value of *50000* is used for DB2, *1433* for Microsoft SQL Server 2005 or Microsoft SQL Server 2008, or *1521* for Oracle.
sdms_jdbc_path	Yes, in these cases: • the *config_sdms* property has the value of *Yes* • the *upgrade* property has the value of *Yes*		X	X	Specifies the fully qualified directory paths where the JDBC driver class files for the SOA Domain Management Server database that is being created are located. To include more than one directory path and JAR file, separate them in the list with a semicolon. For the list of JDBC driver class files required for DB2, Microsoft SQL Server, or Oracle, see "Configuring the SOA Domain Management Server" on page 148. **Important:** When configuring or upgrading an Oracle database (Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2), `ojdbc6.jar` must be used as the JDBC driver. See technote for more information.
sdms_db_create_locally	Yes	*yes* or *no*			Specifies whether the configuration utility must create the SOA Domain Management Server database locally (*yes*) or use an existing (local or remote) SOA Domain Management Server database (*no*). The value must be set to *no* if the database type is Oracle.

Table 20. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
sdms_db_name	No				For DB2 or Microsoft SQL Server databases, this property specifies the name of the SOA Domain Management Server database being created. For DB2, the name can be a maximum of 8 characters. For Microsoft SQL Server, the name can be up to 128 characters. If this property is not specified, the default value of *KD4SDMS* is assumed. **Remember:** If this database exists, it is dropped and re-created. If you do not want to drop an existing database, specify a different name. For Oracle, this parameter is set to the Object System Identifier (SID) that was specified when you ran the `Kd4InitOracleDb` script.
sdms_db_user	Yes if the *config_sdms* property has the value of *Yes*				Specifies the DB2 administrative database user name or the Microsoft SQL Server login name that is authorized to access the SOA Domain Management Server database. For Microsoft SQL Server, the reserved user name of *sa* is not valid. For more information about authorization required for this user, see "Database and User Permissions" on page 115. For Oracle, this property is ignored as *SDMS* is always used as the Oracle user name.
sdms_db_password	Yes if the *config_sdms* property has the value of *Yes*				Specifies the database password associated with the user name specified in the *sdms_db_user* property.
sdms_db_host	Yes, if your SOA Domain Management Server database is on a computer other than where Tivoli Enterprise Portal Server is installed.	Fully qualified host name or *localhost*			Specifies the host name for the database server computer where the SOA Domain Management Server database is located. If your database is on a computer other than where Tivoli Enterprise Portal Server is installed, specify the fully qualified remote host name. If this property is not specified, the default value of *localhost* is used.

Table 20. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
sdms_mssql_instance	No				The property can be used if the value of the **sdms_db_type** property is *mssql2005* or *mssql2008*, and specifies a named instance to be used instead of the default instance. Specify the full instance name, separated from the host name with 2 backslash characters (\\)
tcore_db_type	Yes	*db2* or *oracle*			Specifies the type of database server that is used for the Tivoli Common Object Repository database. When *oracle* is specified, the property sdms_db_type must also be set to *oracle*.
tcore_db_create_locally	Yes	*yes* or *no*			For DB2, this property specifies whether the configuration utility creates the Tivoli Common Object Repository database locally (*yes*) or uses an existing (local or remote) Tivoli Common Object Repository database (*no*). The value must be set to *no* if the database type is Oracle.
tcore_db_host	Yes, if your Tivoli Common Object Repository database is on a computer other than where Tivoli Enterprise Portal Server is installed.	Fully qualified host name or *localhost*			Specifies the host name for the database server computer where the Tivoli Common Object Repository database is located. If your database is on a computer other than where Tivoli Enterprise Portal Server is installed, specify the fully qualified remote hostname. If this property is not specified, the default value of *localhost* is used.
tcore_db_port	No				Specifies the port number for the Tivoli Common Object Repository database. If this property is not specified, the default value of *50000* for a DB2 database or *1521* for an Oracle database is assumed.

Table 20. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
tcore_db_name	No				This property specifies the name of the Tivoli Common Object Repository database. For DB2, if this property is not specified, the default value of *KD4TCORE* is assumed. The name can be a maximum of 8 characters. **Remember:** If you specified to create the database locally and this database exists, it is dropped and recreated. If you do not want to drop an existing database, specify a different name. For Oracle, specify the Oracle System Identifier that was specified when you ran the `make_ora_user` script.
tcore_db_user	Yes, if *config_tcore* has the value of *Yes*				This property specifies the administrative database user name that is authorized to create and access the Tivoli Common Object Repository database. For more information about the authorization required for this user, see "Database and User Permissions" on page 115.
tcore_db_password	Yes, if *config_tcore* or *update_tcore_ auth* has the value of *Yes*				This property specifies the database password associated with the user name specified in the *tcore_db_user* property.

Combining silent operations

When you are installing or upgrading to ITCAM for SOA version 7.2, if you create a silent response file to contain more than one operation (for example, configure Tivoli Common Object Repository and update SOA Domain Management Server), the operations are always performed in the following sequence:

1. Upgrade from version 7.1.1 to 7.2.
2. Configure SOA Domain Management Server
3. Configure Tivoli Common Object Repository
4. Update SOA Domain Management Server authentication credentials
5. Update Tivoli Common Object Repository authentication credentials

When you are updating to ITCAM for SOA version 7.2 Fix Pack 1, if you create a silent response file to contain more than one operation, the operations are always performed in the following sequence:

1. Upgrade from version 7.2 to 7.2 Fix Pack 1.
2. Configure SOA Domain Management Server
3. Configure Tivoli Common Object Repository
4. Update SOA Domain Management Server authentication credentials
5. Update Tivoli Common Object Repository authentication credentials

Some operations are mutually exclusive, and cannot be defined in the same silent response file. These operations can be performed with the same silent response file:

- config_sdms and config_tcore
- update_sdms and config_tcore
- update_sdms and update_tcore
- update_sdms_auth and update_tcore_auth

Silent mode errors and messages

The `ConfigDMS` utility validates the operations and their values in the silent response file and displays a message when required values are missing or when a property is assigned a value that is not valid.

The `ConfigDMS` utility displays messages that describe the operations that are being performed by the utility and results of those operations (success or failure). When an error occurs, the error code and the error message are displayed describing the cause of the failure, if possible.

If the silent response file contains several operations that can be performed from the same file, the first error that occurs stops the `ConfigDMS` utility. For example, if you are configuring both SOA Domain Management Server and Tivoli Common Object Repository and an error occurs during the configuration of SOA Domain Management Server, the SOA Domain Management Server Configuration utility does not start the configuration of Tivoli Common Object Repository.

After the configuration or upgrade of SOA Domain Management Server or Tivoli Common Object Repository completes, you must rebuild and restart the Tivoli Enterprise Portal Server. This reconfiguration can take some time to complete. Be sure to wait for completion before attempting to run the `ConfigDMS` utility again. If you are updating authentication credentials only, you need to restart Tivoli Enterprise Portal Server only.

Increasing the report request limit on the portal server

The report request limit that is specified in the portal server environment file defines the normal limit of pending report requests to the portal server from a single client. This parameter is set to 50 by default. In an IBM Business Process Manager server environment, in particular, if many application servers are monitored on a single application server host, this limit might be exceeded. If you plan to configure data collection for multiple application servers, increase the report request limit to 100.

1. Navigate to the *ITM_Home*`\cnps\kfwenv` file.
2. Add or set the property `KFW_REPORT_REQUEST_LIMIT` to 100. For example:
   ```
   KFW_REPORT_REQUEST_LIMIT=100
   ```
3. Save the changes to the `kfwenv` file.
4. Restart the portal server.

Reconfiguring and restarting the Tivoli Enterprise Portal Server

After the `ConfigDMS` utility completes the tasks of upgrading, configuring, or updating SOA Domain Management Server or Tivoli Common Object Repository, reconfigure Tivoli Enterprise Portal Server.

If you are *updating the authentication credentials* only, you do not have to reconfigure the portal server, but you must restart the portal server for the changes to take effect.

To reconfigure the portal server, complete the following steps:

1. Open the Manage Tivoli Enterprise Monitoring Services console.
2. Verify that the Tivoli Enterprise Portal Server is started.
3. Right-click the Tivoli Enterprise Portal Server component and select **Reconfigure**.
4. When the reconfigure process completes, restart the portal server.

You do not have to reconfigure any of the Tivoli Enterprise Portal Server parameters, so you can accept the current values that are displayed in the configuration steps.

Remember: The first time that you configure SOA Domain Management Server and Tivoli Common Object Repository, reconfiguring the portal server takes at least 5 - 15 minutes to complete, and during this time the Manage Tivoli Enterprise Monitoring Services console might appear to be inoperable.
For more information about rebuilding a DB2 database, see the *IBM DB2 Database for Linux, UNIX, and Windows* Information Center.

Important:

- If your Tivoli Enterprise Portal Server is running on a Windows 2008 operating system and is using a DB2 database, you must rebuild the Tivoli Enterprise Portal Server DB2 database after reconfiguring and restarting the Tivoli Enterprise Portal Server.
- If any of the ITCAM for SOA workspaces are not available, you must rebuild the Tivoli Enterprise Portal Server database.

To rebuild the database, complete the following steps:

1. Open the Manage Tivoli Enterprise Monitoring Services console.
2. Right-click the Tivoli Enterprise Portal Server component and select **Advanced** -> **Utilities** -> **Build TEPS database**.

Chapter 5. Configuring topology support on Linux systems

Topology support provides views of service-to-service relationships and the relationship between services and service registry information and business process information.

Overview

ITCAM for SOA supports the discovery, storage, and display of information about service resources (application servers, service ports, and operations) and the relationships between them. These service-to-service relationships and flows can then be displayed in Tivoli Enterprise Portal topology workspaces and views.

ITCAM for SOA provides two key components for this topology support:

SOA Domain Management Server
Stores information about service resources and service-to-service relationships and flows. It can retrieve service registry and business process integration information from the Tivoli Common Object Repository, if present, to display this information in topology workspaces and views.

Tivoli Common Object Repository
Stores service registry and business processes integration topology data that is retrieved from one or more discovery library adapters.

Installing and configuring topology support

To install and configure topology support for ITCAM for SOA version 7.2 fix pack 1, complete the following steps:

1. Create the SOA Domain Management Server database on the Tivoli Enterprise Portal Server (or remotely on a different server).

   Use the database creation scripts that come with ITCAM for SOA and start the database. If you are using a DB2 database, you can create the database with the SOA Domain Management Server Configuration utility. If you are using an Oracle database, you must create the database manually.
2. (Optional) Create the Tivoli Common Object Repository database on the Tivoli Enterprise Portal Server (or remotely on a different server).

   Use the database creation scripts that come with ITCAM for SOA and start the database. If you are using a DB2 database, you can create the database with the SOA Domain Management Server Configuration utility. If you are using an Oracle database, you must create the database manually.
3. Run the SOA Domain Management Server Configuration utility.

   If you created the databases already, select the option to use an existing database and complete the configuration of the database.

   If you did not create the databases already, select the option to create each database locally and complete the configuration of the database.
4. Rebuild and restart the Tivoli Enterprise Portal Server.

Upgrading or updating topology support

To upgrade topology support to ITCAM for SOA version 7.2 or update topology support to ITCAM for SOA version 7.2 fix pack 1, complete the following steps:

1. Verify that the SOA Domain Management Server database and the Tivoli Common Object Repository database (if installed) are started.
2. If the SOA Domain Management Server or the Tivoli Common Object Repository are on a remote server, run the migration scripts that are provided by ITCAM for SOA.
3. Run the SOA Domain Management Server Configuration utility to perform the upgrade.

   If the databases are located remotely, run the utility with the `-remoteSDMS` or the `-remoteTCORE` arguments.
4. Rebuild and restart the Tivoli Enterprise Portal Server.

Detailed instructions on how to complete each of the upgrade steps are provided in the following sections.

Important: If you are upgrading from ITCAM for SOA version 7.1.1, you must upgrade topology support to ITCAM for SOA version 7.2 before you update topology support to version 7.2 fix pack 1.

Topology Views and Configuration Options

When planning your installation, consider the following points:

- Whether to install the SOA Domain Management Server and Tivoli Common Object Repository components.
- Whether to use an existing or new database for each component.
- Whether the databases will reside on a remote server or locally on the portal server.
- What type of database to use.

Topology Views

The topology components that you must install and configure depend on the topology views you want to display:

Table 21. Topology Views

Service-to-Service Topology Views	Service Registry and Business Process Integration Topology Views	Components Required
Yes	No	SOA Domain Management Server
Yes	Yes	SOA Domain Management Server and Tivoli Common Object Repository
No	Yes	SOA Domain Management Server and Tivoli Common Object Repository

Restriction: To display service-to-service topology views or service registry and business progress integration topology views, or both, when you integrate ITCAM for SOA version 7.2 or later with Tivoli Monitoring version 6.2.2, you must install SOA Domain Management Server and Tivoli Common Object Repository.

If you decide to configure only SOA Domain Management Server, create a database for SOA Domain Management Server that is not used by other applications.

If you decide to configure the SOA Domain Management Server and the Tivoli Common Object Repository, the following configuration options are available:

1. Use an existing database that is used by other applications for SOA Domain Management Server and Tivoli Common Object Repository.
2. Create a database for SOA Domain Management Server, and create a separate new database for Tivoli Common Object Repository.
3. Create a database that is shared by both SOA Domain Management Server and Tivoli Common Object Repository. This option is only available when you create the database manually.

Both the SOA Domain Management Server component and the Tivoli Common Object Repository component use either a local or remote database to contain their service resource and topology data. You have the option of configuring the SOA Domain Management Server to operate with or without Tivoli Common Object Repository.

SOA Domain Management Server Configuration Options

If you use an existing database for SOA Domain Management Server and, optionally, for Tivoli Common Object Repository you must run the SOA Domain Management Server Configuration Utility to configure topology support on both components.

If you create a SOA Domain Management Server database manually on the local portal server or on a remote database server, the configuration options that are listed in the following table are available.

Table 22. Options for manually configuring the database server for SOA Domain Management Server

Location	Database Type	Topic
Local	DB2	“Manually creating a DB2 database locally on Linux or UNIX systems for SOA Domain Management Server” on page 185
Local	Oracle	“Manually creating an Oracle database locally on Linux or UNIX systems for SOA Domain Management Server” on page 185
Remote	DB2	“Manually creating a DB2 database remotely on Linux or UNIX systems for SOA Domain Management Server” on page 187
Remote	Oracle	“Manually creating an Oracle database remotely on Linux or UNIX systems for SOA Domain Management Server” on page 188

Tip: If this server is installed on the same computer as the portal server, the database server is usually the same database server that is used by the portal server.

Tivoli Common Object Repository Configuration Options

If you manually create a new Tivoli Common Object Repository database, the configuration options that are listed in the following table are available:

Table 23. Options for manually configuring the database server for Tivoli Common Object Repository

Location	Database Type	Topic
Local	DB2	“Manually creating a DB2 database locally on Linux or UNIX systems for Tivoli Common Object Repository” on page 190
Local	Oracle	“Manually creating an Oracle database locally on Linux or UNIX systems for Tivoli Common Object Repository” on page 190
Remote	DB2	“Manually creating a DB2 database remotely on Linux or UNIX systems for the Tivoli Common Object Repository” on page 192
Remote	Oracle	“Manually creating an Oracle database remotely on Linux or UNIX systems for Tivoli Common Object Repository” on page 193

Important: You require database administrative authority to create the databases that are used with SOA Domain Management Server and Tivoli Common Object Repository. For more information about database permissions, see “Database and User Permissions.”

Planning topology support on Linux or UNIX

Before you configure SOA Domain Management Server and the optional Tivoli Common Object Repository, you must have enough available space on the partition where Tivoli Monitoring is installed. You must know the permissions that are required for creating and configuring the SOA Domain Management Server and Tivoli Common Object Repository databases and the permissions required for the user that is specified as the database administrator.

Minimum space requirements on the file system

Before you configure SOA Domain Management Server and optional Tivoli Common Object Repository, you must have enough available space on the partition where Tivoli Monitoring is installed. When you configure SOA Domain Management Server and optional Tivoli Common Object Repository, you must accommodate the files needed for these components, including room for growth for Tivoli Common Object Repository bulk load results files.

For more information about the required hardware for ITCAM for SOA, see “Required hardware” on page 16.

Database and User Permissions

When you run the SOA Domain Management Server Configuration Utility (referred to by its script name, `ConfigDMS`), you must have certain minimum user permissions, depending on the task that you are doing.

Permissions required when installing SOA Domain Management Server or Tivoli Common Object Repository

You require the following permissions when you configure the SOA Domain Management Server and Tivoli Common Object Repository database as part of installing ITCAM for SOA.

DB2 database configuration permissions

The permissions that are required when configuring a DB2 database for SOA Domain Management Server and Tivoli Common Object Repository as part of an installation of ITCAM for SOA are in Table 24:

Table 24. Permissions required when configuring a DB2 database

Task	User and Database Requirements
Permissions required to run the scripts to manually create a DB2 database either locally or remotely	The requirements are as follows: • The user must belong to the DB2 instance administrative group (for example, db2grp1). • When creating an SOA Domain Management Server database, user must have permission to read and run the `kd4MakeDB2db.sh` script and write permission for the directory that contains the script. • When creating an Tivoli Common Object Repository database, user must have permission to read and run the `make_db2_db.sh` script and write permission for the directory that contains the script.

Table 24. Permissions required when configuring a DB2 database (continued)

Task	**User and Database Requirements**
Permissions required to run the ConfigDMS utility to either (a) configure a DB2 database that was configured locally or remotely, or (b) create the DB2 database locally and configure it	The requirements are as follows: • The user must be the user who installed IBM Tivoli Monitoring (root or db2inst1). • The user must have permission to rebuild, restart, and run Tivoli Enterprise Portal Server • The user must have read, write, and modify permissions for the following directories: – *ITM_HOME*/*platform*/cq directory and its subdirectories – *ITM_HOME*/*platform*/iw directory and its subdirectories – *ITM_HOME*/config directory and its subdirectories – *ITM_HOME*/logs directory and its subdirectories • If you are running the ConfigDMS utility as the root user, your root user must also have the following capabilities: – The user must be able to source the DB2 instance profile. – The user must be authorized to issue the following command: su - *DB_USER* In this command, *DB_USER* refers to the database administrator user that is configured for SOA Domain Management Server with the ConfigDMS utility. The user specified by *DB_USER* must have read, write, and execute permission for the *ITM_Home*/*platform*/cq/Products/KD4/latest/bin directory. If your database administrator user does not have read, write, and execute permissions for these directories, you can use the following alternative procedure to create the database manually: 1. When configuring SOA Domain Management Server, complete the following steps: a. Copy the kd4RemoteDB.tar.gz file from the *ITM_Home*/*platform*/cq/Products/KD4/latest/db directory on the computer where the DB2 administrator has read, write, and execute permission and extract the files. b. Run the kd4MakeDB2db.sh script while logged in as the database administrator. 2. When configuring Tivoli Common Object Repository, complete the following steps: a. Copy the make_db2_db.sh file from the *ITM_HOME*/*platform*/cq/Products/KD4/latest/tcore/db directory to a local directory on the computer where the DB2 administrator has read, write, and execute permissions. b. Run the make_db2_db.sh script while logged in as the database administrator. 3. Run the ConfigDMS utility as the user who installed Tivoli Monitoring and select the option to use an existing database. For more information about manually creating the database, see "Creating the SOA Domain Management Server database" on page 184 for SOA Domain Management Server and see "Creating the Tivoli Common Object Repository database" on page 189 for Tivoli Common Object Repository.

Table 24. Permissions required when configuring a DB2 database (continued)

Task	User and Database Requirements
Requirements for database administrator user specified using the ConfigDMS utility	The requirements are as follows: • The user must be a DB2 administrator user (for example, *db2inst1*). Alternatively, the user might be a database user specific to the database with at least the authorization to complete the following tasks: – Connect to the database. – Create tables. – Perform select, insert, update, and delete operations on the tables in the database. • The user is the same user as specified by *DB_USER* in the following command: `su - DB_USER` • DB2 profile must be automatically sourced when you log in as this user. The user is used by the SOA Domain Management Server or Tivoli Common Object Repository to access the database at run time. The SOA Domain Management Server user name is not to be used as the database schema name. The schema name is hardcoded to *SDMS*. The Tivoli Common Object Repository user name is used as the database schema name.

Oracle database configuration permissions

The permissions that are required when configuring an Oracle database for SOA Domain Management Server and Tivoli Common Object Repository as part of an installation of ITCAM for SOA are in Table 25:

Table 25. Permissions required when configuring an Oracle database

Task	User and Database Requirements
Permissions required to run the `KD4InitOracleDb.sh` script.	The requirements are as follows: • The user who created the SOA Domain Management Server database must have read, write, and execute permissions for the directory on the local server or the remote server containing the `KD4InitOracleDb.sh`. • The script must be run as the user who created the SOA Domain Management Server database.
Permissions required to run the `make_ora_user.sh` script.	The requirements are as follows: • The user who created the Tivoli Common Object Repository database must have read, write, and execute permissions for the directory on the local server or the remote server that contains the `make_ora_user.sh` script. • The script must be run as the user who created the Tivoli Common Object Repository database.
Requirements for database user specified when running the `KD4InitOracleDb.sh` script.	The user name and schema are hardcoded as *SDMS*. If the user exists, it is dropped and re-created by the script.
Requirements for database user specified when running the `make_ora_user.sh` script.	The requirements are as follows: • If the user exists, it is dropped and re-created by the script. • Do not specify *SDMS* as the user name when running the script. The user name is also used as the schema name.

Table 25. Permissions required when configuring an Oracle database (continued)

Task	User and Database Requirements
Permissions required to run the ConfigDMS utility to configure an Oracle database that is installed locally or remotely	The requirements are as follows: • The user must be the user who installed IBM Tivoli Monitoring. • The user must have permission to rebuild, restart, and run the Tivoli Enterprise Portal Server. • The user must have read, write, and modify permissions for the following directories: – *ITM_HOME*/*platform*/cq directory and its subdirectories – *ITM_HOME*/*platform*/iw directory and its subdirectories – *ITM_HOME*/config directory and its subdirectories – *ITM_HOME*/logs directory and its subdirectories For information about resolving directory path and platform variables, see "Resolving directory path variables" on page xvi.
Requirements for database administrator user specified with the ConfigDMS utility	The requirements for the SOA Domain Management Server are: • The SOA Domain Management Server Oracle user name is hardcoded to *SDMS*. • The SOA Domain Management Server Oracle user password must be the same as the password specified when you ran the kd4InitOracleDb.sh script. • The password cannot contain the '$' symbol. The requirements for the Tivoli Common Object Repository are: • The Tivoli Common Object Repository Oracle user name must be the same as the user name specified when you ran the Oracle make_ora_user.sh script. • The Tivoli Common Object Repository Oracle user password must be the same as the password specified when you ran the make_ora_user.sh script.

Permissions required when upgrading to ITCAM for SOA V7.2 or updating to ITCAM for SOA V7.2 Fix Pack 1

Before you upgrade or update topology support, review the permissions required for configuring SOA Domain Management Server and Tivoli Common Object Repository local databases when performing the following tasks:

- Upgrading ITCAM for SOA from version 7.1.1 (all releases) to version 7.2.
- Migrating remote databases from version 7.1.1.3 to version 7.2.
- Updating ITCAM for SOA from version 7.2 to version 7.2 Fix Pack 1.

The permissions required are outlined in the following sections.

DB2 database upgrade permissions

The permissions that are required when migrating a DB2 database for SOA Domain Management Server and Tivoli Common Object Repository are in Table 26 on page 183.

Table 26. Permissions required when upgrading a DB2 database

Task	**User and Database Requirements**
Permissions required to run the `ConfigDMS` utility to upgrade the DB2 database	The requirements are as follows: • The user must be the user who installed IBM Tivoli Monitoring (root or db2inst1). • The user must have permission to rebuild, restart, and run Tivoli Enterprise Portal Server. • The user must have read, write, and modify permissions for the following directories: – *ITM_HOME*/*platform*/`cq` directory and its subdirectories – *ITM_HOME*/*platform*/`iw` directory and its subdirectories – *ITM_HOME*/`config` directory and its subdirectories – *ITM_HOME*/`logs` directory and its subdirectories • If you are running the `ConfigDMS` utility as the root user, your root user must also have the following capabilities: – The user must be able to source the DB2 instance profile. – The user must be authorized to issue the following command: `su - DB_USER` In this command, *DB_USER* refers to the database administrator user that was configured as the SOA Domain Management Server or Tivoli Common Object Repository database user in ITCAM for SOA version 7.1.1. The user specified by *DB_USER* must have read, write, and execute permissions for the *ITM_HOME*/*platform*/`cq/Products/KD4/latest/bin` directory when upgrading SOA Domain Management Server or *ITM_HOME*/*platform*/`cq/Products/KD4/latest/tcore/bin` directory when upgrading Tivoli Common Object Repository.
Permissions required to run the `kd4MigrateDB2db.sh` script to migrate a remote SOA Domain Management Server database	The requirements are as follows: • The user who created the SOA Domain Management Server database must have read, write, and execute permissions for the directory on the remote server that contains the `kd4MigrateDB2db.sh` script. Also, the user must have permission to invoke the database tools. • The script must be run as the user who created the SOA Domain Management Server database. • The user who runs the `kd4MigrateDB2db.sh` script must have read permissions for all other files in the directory on the remote server that contains the script, for example, `kd4version.properties` and `kd4ConfigSDMSUtilties.sh`. • The user who runs the `kd4MigrateDB2db.sh` script must have the necessary permissions to invoke the database tools.

Oracle database upgrade permissions

The permissions that are required when migrating an Oracle database for SOA Domain Management Server and Tivoli Common Object Repository are in Table 27 on page 184:

Table 27. Permissions required when upgrading an Oracle database

Task	User and Database Requirements
Permissions required to run the ConfigDMS utility to upgrade an Oracle database that is installed locally or remotely	The requirements are as follows: • The user must be the user who installed IBM Tivoli Monitoring. • The user must have permission to rebuild, restart, and run the Tivoli Enterprise Portal Server. • The user must have read, write, and modify permissions for the following directories: – *ITM_HOME*/*platform*/cq directory and its subdirectories – *ITM_HOME*/*platform*/iw directory and its subdirectories – *ITM_HOME*/config directory and its subdirectories – *ITM_HOME*/logs directory and its subdirectories • The user must be able to source the usr/local/bin/oraenv file. For information about resolving directory path and platform variables, see "Resolving directory path variables" on page xvi.
Permissions required to run the kd4MigrateOracledb.sh to upgrade an Oracle database that is installed remotely.	The user who runs the kd4MigrateOracledb.sh script must have read, write, and execute permissions for the directory on the remote server that contains the kd4MigrateOracledb.sh script. The user must be able to source the usr/local/bin/oraenv file.

Creating the SOA Domain Management Server database

The SOA Domain Management Server database can be created on a supported DB2 server or Oracle server.

When creating the SOA Domain Management Server database, the following options are available:

- Let the SOA Domain Management Server Configuration utility create and configure the SOA Domain Management Server database locally for you on your portal server computer.
- Manually create a database on the local portal server before running the SOA Domain Management Server Configuration utility.
- Manually create a database on a remote database server before running the SOA Domain Management Server Configuration utility.

Restriction: If an Oracle database is used for the SOA Domain Management Server, it must be created manually before running the SOA Domain Management Server Configuration utility.

If this database server is installed on the same computer as the portal server, the database server is usually the same database server that is used by the portal server.

Manually creating a local SOA Domain Management Server database

To create and configure the SOA Domain Management Server database locally, use the scripts found in the *TEPS_HOME*/Products/KD4/latest/bin directory on the computer where the portal server is installed.

You can use either a DB2 or Oracle database to create the SOA Domain Management Server database.

When the database is created or installed locally with the scripts provided, you must run the `ConfigDMS` utility to configure the database. From the `ConfigDMS` utility, choose the option to use an existing database. When the database is configured, you must rebuild and restart the Tivoli Enterprise Portal Server.

The next section presents the options for creating the SOA Domain Management Server database.

Manually creating a DB2 database locally on Linux or UNIX systems for SOA Domain Management Server

To manually create the DB2 database locally, complete these steps:

1. Verify that your user name belongs to the DB2 instance administrative group (for example, db2grp1).
2. Source the DB2 instance profile by performing the following steps:
   - Navigate to `/home/`*`dbuser`*`/sqllib`, where *dbuser* is the DB2 instance user name (for example, db2inst1).
   - Run the following command:

     ```
     . ./db2profile
     ```

     Remember: Be sure to leave a space between the first period and the **`./dbprofile`** command.
3. Navigate to the *`ITM_Home`*`/`*`platform`*`/cq/Products/KD4/latest/bin` directory.

   For more information about resolving directory path and platform variables, see "Resolving directory path variables" on page xvi.
4. Verify that your user name has permission to read and execute the `kd4MakeDB2db.sh` script and write permission for the directory that contains the script.
5. Run the `kd4MakeDB2db.sh` script and provide a name for the SOA Domain Management Server database, such as `KD4SDMS`. The name can have a maximum of 8 characters. For example:

   ```
   ./kd4MakeDB2db.sh KD4SDMS
   ```

   Tip: If this database exists on the local system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.

   Note: The password cannot contain the '$' symbol.
6. Wait for the database creation process to complete.

   The script verifies the database version and displays a message if the version is unsupported. The output generated by this script is written to a file called createDB2DBResults.txt in the same directory where the script is run. See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with any errors that you encounter.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 178.

Manually creating an Oracle database locally on Linux or UNIX systems for SOA Domain Management Server

The Oracle database that you use for SOA Domain Management Server must meet the following requirements:

- The Oracle database must be created with Unicode (AL32UTF8) as the database character set.
- The Oracle database must be created with UTF8 as the national character set.

To manually create the Oracle database locally on Linux or UNIX systems, complete the following steps:

1. Install Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 on the portal server.
2. Use the Database Configuration Assistant (DBCA) to create a database locally for the SOA Domain Management Server. For specific instructions on how to create the Oracle database, refer to your Oracle database documentation.
3. Ensure that you are logged in as the user who created the Oracle database for the SOA Domain Management Server.
4. Start the Oracle listener with the Oracle Listener Service.
5. Navigate to the *ITM_Home/platform*/cq/Products/KD4/latest/bin directory and verify that your user name has permission to read and issue the kd4InitOracleDb.sh script, the kd4InitOracleDB_user.sql file, and the sdms_oracle.sql file. Verify that your user name has write permission for that directory.
6. Run the kd4InitOracleDb.sh script to create the SOA Domain Management Server user, create the SOA Domain Management Server role, grant authorities, and create the schema. The name of the Oracle user and the name of the schema are hardcoded as SDMS. Use this syntax:

   ```
   kd4InitOracleDb.sh  SID ORACLE_HOME USER_PW SYS_PW
   ```

   Where:

   SID Specifies the Oracle System Identifier (SID) for the SOA Domain Management Server database.

   ORACLE_HOME
   Specifies the directory where the Oracle database server is installed, for example, /u01/app/oracle/product/11.1.0/db_1.

   If the *ORACLE_HOME* environment variable is set, you can provide it as the value for this parameter.

   Tip: Ensure that the directory path does not end with a backslash (\).

   USER_PW
   Specifies the password for the Oracle SOA Domain Management Server user created by the kd4InitOracleDb.sh script. The password cannot contain the '$' symbol.

   SYS_PW
   Specifies the password for the *SYS* user.

   The *SYS* user is created automatically when you create an Oracle database.
7. Wait for the kd4InitOracleDb.sh script to complete.

   Remember: If an Oracle user called SDMS exists, it can take some time to drop the user and re-create it. During this time, the script can seem to hang.

The results of the kd4InitOracleDb.sh script are written to the initOracleDBresults.txt file.

If errors occur while running the Kd4InitOracleDb.sh script, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more details.

For information about database and user permissions when creating and configuring topology databases, see “Database and User Permissions” on page 178.

Manually creating a remote SOA Domain Management Server database

To create and configure the SOA Domain Management Server DB2 or Oracle database remotely, copy the kd4RemoteDB.tar.gz file from the *TEPS_Home*/Platform/cq/Products/KD4/latest/db directory (on the computer where your portal server is installed) to the remote computer where you plan to create the SOA Domain Management Server database. Extract this file into any directory and run the provided scripts to create the database as needed.

On Linux or UNIX systems, use the following command to extract the file:

```
tar -xzvf kd4RemoteDB.tar.gz
```

The **tar** command for AIX operating systems does not support the –z option to extract files from a tar.gz file. If you are using the AIX operating system, download the gunzip utility, which you can use to extract files from a .tar.gz file.

Restriction: The kd4RemoteDB.tar.gz file is only available after ITCAM for SOA application support is installed.

When the database is created or installed remotely with the scripts, you must run the ConfigDMS utility with the -remoteSDMS argument to configure the database. From the ConfigDMS utility, choose the option to use an existing database. When the database is configured, you must rebuild and restart the Tivoli Enterprise Portal Server.

Manually creating a DB2 database remotely on Linux or UNIX systems for SOA Domain Management Server

To manually create a DB2 database on a remote server, complete these steps:

1. Log in to the remote computer as a user that belongs to the DB2 instance administrative group (for example, db2grp1).
2. Source the DB2 instance profile by performing the following steps:
   - Navigate to /home/*dbuser*/sqllib, where *dbuser* is the DB2 instance user name (for example, db2inst1).
   - Run the command:

     ```
     . ./db2profile
     ```

     Tip: Be sure to leave a space between the first period and the **./dbprofile** command.
3. Navigate to the directory on the remote computer where you copied the kd4MakeDB2db.sh script.
4. Verify that your user name has permission to read and issue the kd4MakeDB2db.sh script and write permission for the directory that contains the script.
5. Run the kd4MakeDB2db.sh script and provide a name for the SOA Domain Management Server database, such as KD4SDMS. The name can have a maximum of 8 characters. For example:

   ```
   ./kd4MakeDB2db.sh KD4SDMS
   ```

Remember: If this database exists on the remote system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.

Note: The password cannot contain the '$' symbol.

6. Wait for the database creation process to complete.

   The script verifies the database version and displays a message if it is at an unsupported level. The output generated by this script is written to a file called `createDB2DBResults.txt` in the same directory where the script is run. See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with any errors that you encounter.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 178.

Manually creating an Oracle database remotely on Linux or UNIX systems for SOA Domain Management Server

The Oracle database that you use for SOA Domain Management Server must meet these requirements:

- The Oracle database must be created with Unicode (AL32UTF8) as the database character set.
- The Oracle database must be created with UTF8 as the national character set.

To manually create the Oracle database on a remote server, complete these steps:

1. Install an Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 database server on the remote server.
2. Use the Database Configuration Assistant (DBCA) to create a database on the remote server for the SOA Domain Management Server. For specific instructions on how to create the Oracle database, refer to your Oracle database documentation.
3. Ensure that you are logged in as the user who created the Oracle database for the SOA Domain Management Server.
4. Start the Oracle listener with the Oracle Listener Service.
5. Navigate to the directory on the remote computer where you extracted the `kd4RemoteDB.tar.gz` file, and verify that your user name has permission to read and issue the `kd4InitOracleDb.sh` command, the `kd4InitOracleDB_user.sql` file, and the `sdms_oracle.sql` file. Verify that your user name has write permission for that directory.
6. Run the `kd4InitOracleDb.sh` script to create the SOA Domain Management Server user, create the SOA Domain Management Server role, grant authorities, and create the schema. The name of the Oracle user and the name of the schema is hardcoded as `SDMS`. Use this syntax:

   ```
   kd4InitOracleDb.sh  SID ORACLE_HOME USER_PW SYS_PW
   ```

   Where:

   SID Specifies the Oracle System Identifier (SID) for the SOA Domain Management Server database.

   ORACLE_HOME
   Specifies the directory where the Oracle database server is installed, for example, `/u01/app/oracle/product/11.1.0/db_1`.

   If the `ORACLE_HOME` environment variable is set, you can provide it as the value for this parameter.

Tip: Ensure that the directory path does not end with a backslash (\).

USER_PW
Specifies the password for the Oracle SOA Domain Management Server user created by the `kd4InitOracleDb.sh` script.

SYS_PW
Specifies the password for the `SYS` user. The password cannot contain the '$' symbol.

The `SYS` user is created automatically when you create an Oracle database.

7. Wait for the `kd4InitOracleDb.sh` script to complete.

   Remember: If an Oracle user called SDMS exists, it can take some time to drop the user and re-create it. During this time, the script can appear to hang.

The results of the `kd4InitOracleDb.sh` script are written to the `initOracleDBresults.txt` file.

If errors occur while running the `Kd4InitOracleDb.sh` script, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more details.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 178.

Creating the Tivoli Common Object Repository database

The Tivoli Common Object Repository database can be created on a supported DB2 server or Oracle server.

When creating the Tivoli Common Object Repository database, you have the following options:

- Let the SOA Domain Management Server Configuration utility create and configure the Tivoli Common Object Repository database locally for you on your portal server computer.
- Manually create a database on the local portal server before running the SOA Domain Management Server Configuration utility.
- Manually create a database on a remote database server before running the SOA Domain Management Server Configuration utility.

Restriction: If an Oracle database is used for the Tivoli Common Object Repository, it must be created manually before running the SOA Domain Management Server Configuration utility.

If this database server is installed on the same computer as the portal server, the database server is usually the same database server that is used by the portal server.

Manually creating a local Tivoli Common Object Repository database

To create and configure the Tivoli Common Object Repository DB2 database locally, use the `make_db2_db.sh` script found in the *`ITM_Home`*`/`*`platform`*`/cq/Products/KD4/latest/tcore/db/` directory on the computer where the portal server is installed.

Important: This script creates the Tivoli Common Object Repository database but does not create the database schema or tables. The schema and tables are created when you run the SOA Domain Management Server Configuration utility to configure Tivoli Common Object Repository.

To configure an Oracle database for Tivoli Common Object Repository, manually create the database using Oracle's Database Configuration Assistant and use the `make_ora_user.sh` found in the *ITM_Home*/*platform*/`cq/Products/KD4/latest/tcore/db/` directory to create user roles and grant authorities.

When the database is created or installed locally with the scripts provided, you must run the `ConfigDMS` utility to configure the database. From the `ConfigDMS` utility, choose the option to use an existing database. When the database is configured, you must rebuild and restart the Tivoli Enterprise Portal Server.

Manually creating a DB2 database locally on Linux or UNIX systems for Tivoli Common Object Repository

To manually create the DB2 database locally, complete these steps:

1. Verify that your user name belongs to the DB2 instance administrative group (for example, db2grp1).
2. Source the DB2 instance profile by performing the following steps:
   a. Navigate to `/home/`*dbuser*`/sqllib`, where *dbuser*is the DB2 instance user name (for example, db2inst1).
   b. Run the command:
      ```
      . ./db2profile
      ```
      Tip: Be sure to leave a space between the first period and the **`./dbprofile`** command.
3. Navigate to the *ITM_Home*/*platform*/`cq/Products/KD4/latest/tcore/db/` directory.

   For more information about resolving directory path and platform variables, see "Resolving directory path variables" on page xvi.
4. Run the `make_db2_db.sh` script and provide a name for the Tivoli Common Object Repository database, such as `KD4TCORE`. The name can have a maximum of 8 characters. For example:
   ```
   ./make_db2_db.sh KD4TCORE
   ```
   Remember: If this database exists on the local system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.
   Verify that your user name has permission to read and execute the `make_db2_db.sh` script and write permission for the directory that contains the script.
5. Wait for the database creation process to complete.

   See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with any errors that you might encounter.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 178.

Manually creating an Oracle database locally on Linux or UNIX systems for Tivoli Common Object Repository

The Oracle database that database you use for Tivoli Common Object Repository must meet these requirements:

- The Oracle database must be created with Unicode (AL32UTF8) as the database character set.
- The Oracle database must be created with UTF8 as the national character set.

Important: If you use an Oracle database for Tivoli Common Object Repository, it is recommended that you also use an Oracle database for SOA Domain Management Server.

To manually create the Oracle database locally, complete these steps:

1. Install Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 on the portal server.
2. Use the Database Configuration Assistant (DBCA) to create a database locally for the Tivoli Common Object Repository. For specific instructions on how to create the Oracle database, refer to your Oracle database documentation.
3. Ensure that you are logged in as the user who created the Oracle database for the Tivoli Common Object Repository.
4. Ensure the *ORACLE_HOME* environment variable is set to the directory where your Oracle database server is installed.
5. Start the Oracle listener with the Oracle Listener Service.
6. Navigate to the `ITM_Home/platform/cq/Products/KD4/latest/tcore/bin` directory and verify that your user name has read, write, and execute permissions for that directory.
7. Verify that your user name has permission to read and execute the `make_ora_user.sh` script and write permission for the directory that contains the script.
8. Use this syntax to run the `make_ora_user.sh` script:

   ```
   make_ora_user.sh  SID USER_NAME USER_PW
   ```

   Where:

   SID Specifies the Oracle System Identifier (SID) for the Tivoli Common Object Repository database.

   USER_NAME
   Specifies the name of the Oracle user that is created by the script `make_ora_user.sh`.

   Tip: Do not specify `SDMS` as the user name when running the script.

   The name is also used as the schema name. If the Oracle user exists, it is dropped and re-created by the script.

   USER_PW
   Specifies the password for the Oracle Tivoli Common Object Repository user created by the script.

   Important: The `make_ora_user.sh` script also accepts optional parameters for the archive user name and password. You must not enter these parameter values when configuring Tivoli Common Object Repository.
9. Wait for the `make_ora_user.sh` script to complete.

If errors occur while running the `make_ora_user.sh` script, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more details.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 178.

Manually creating a remote Tivoli Common Object Repository database

To create and configure the Tivoli Common Object Repository DB2 database remotely, you need to copy the `make_db2_db.sh` script found in the *TEPS_Home*/`Platform/cq/Products/KD4/latest/db` directory (on the computer where your Tivoli Enterprise Portal Server is installed) to the remote computer where you plan to create the Tivoli Common Object Repository database, and run this script to create the database.

Important: This script creates the Tivoli Common Object Repository database but does not create the database schema or tables. The schema and tables are created when you run the SOA Domain Management Server Configuration utility to configure Tivoli Common Object Repository.

To configure an Oracle database for Tivoli Common Object Repository remotely, manually create the database with the Oracle Database Configuration Assistant on the remote computer. Copy the `make_ora_user.sh` script in the *TEPS_Home*/`Platform/cq/Products/KD4/latest/db` directory to the remote computer where you plan to create the Tivoli Common Object Repository database, and run this script to create user roles and grant authorities.

When the database is created or installed remotely with the scripts provided, you must run the `ConfigDMS` utility with the `-remoteTCORE` argument to configure the database. From the `ConfigDMS` utility, choose the option to use an existing database. When the database is configured, you must rebuild the Tivoli Enterprise Portal Server.

Manually creating a DB2 database remotely on Linux or UNIX systems for the Tivoli Common Object Repository

To run the script on the remote computer for DB2, complete these steps:

1. Log in to the remote computer as a user that belongs to the DB2 instance administrative group (for example, db2grp1).
2. Source the DB2 instance profile by performing the following steps:
   a. Navigate to `/home/`*`dbuser`*`/sqllib`, where *dbuser* is the DB2 instance user name (for example, db2inst1).
   b. Run the command:
      ```
      . ./db2profile
      ```
      Tip: Be sure to leave a space between the first period and the **`./dbprofile`** command.
3. Navigate to the directory on the remote computer where you copied the `make_db2_db.sh` script.
4. Verify that your user name has permission to read and execute the `make_db2_db.sh` script and write permission for the directory that contains the script.
5. Run the `kdrMakeDB2db.sh` script and provide a name for the Tivoli Common Object Repository database, such as `KD4TCORE`. The name can have a maximum of 8 characters. For example:
   ```
   ./make_db2_db.sh KD4TCORE
   ```

Remember: If this database exists on the remote system, it is dropped and re-created. If you do not want to drop an existing database, specify a different name.

6. Wait for the database creation process to complete.

   The script verifies the database version and displays a message if the version is unsupported. The output generated by this script is written to a file called `createDB2DBResults.txt` in the same directory where the script is run. See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with any errors that you encounter.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 178.

Manually creating an Oracle database remotely on Linux or UNIX systems for Tivoli Common Object Repository

The Oracle database that you use for the Tivoli Common Object Repository must meet these requirements:

- The Oracle database must be created with Unicode (AL32UTF8) as the database character set.
- The Oracle database must be created with UTF8 as the national character set.

Important: If you use an Oracle database for Tivoli Common Object Repository, it is recommended that you also use an Oracle database for SOA Domain Management Server.

To manually create the Oracle database on a remote server, complete these steps:

1. Install Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2 on a remote server.
2. Use the Database Configuration Assistant (DBCA) to create a database remotely for the Tivoli Common Object Repository. For specific instructions on how to create the Oracle database, refer to your Oracle database documentation.
3. Ensure the `$ORACLE_HOME` environment variable is set to the directory where your Oracle database server is installed.
4. Start the Oracle listener with the Oracle Listener Service.
5. Navigate to the directory on the remote computer where you copied the `make_ora_user.sh` script.
6. Verify that your user name has permission to read and run the `make_ora_user.sh` script and write permission for the directory that contains the script.
7. Use this syntax to run the `make_ora_user.sh` script:

   ```
   make_ora_user.sh  SID USER_NAME USER_PW
   ```

   Where:

   SID Specifies the Oracle System Identifier (SID) for the Tivoli Common Object Repository database.

   USER_NAME
   Specifies the name of the Oracle user that is created by the script `make_ora_user.sh`.

   Tip: Do not specify `SDMS` as the user name when running the script.

   The name is also used as the schema name. If the Oracle user exists, it is dropped and re-created by the script.

USER_PW
Specifies the password for the Oracle Tivoli Common Object Repository user created by the script.

Important: The make_ora_user.sh script also accepts optional parameters for the archive user name and password. You must not enter these parameter values when configuring Tivoli Common Object Repository.

8. Wait for the make_ora_user.sh script to complete.

If errors occur while running the make_ora_user.sh script, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more details.

For information about database and user permissions when creating and configuring topology databases, see "Database and User Permissions" on page 178.

Running the ConfigDMS utility

ITCAM for SOA provides the SOA Domain Management Server Configuration utility (referred to as ConfigDMS) that simplifies the configuration of SOA Domain Management Server and Tivoli Common Object Repository topology support. The utility runs in either a graphical user interface mode or in console mode. A silent configuration method is also supported, and optional logging controls are provided to help you diagnose problems.

In addition to configuring topology support, you can use the ConfigDMS utility to create SOA Domain Management Server and Tivoli Common Object Repository DB2 or Microsoft SQL Server databases locally.

If preferred, you can use the database creation scripts provided with the product to create local or remote databases.

Restriction: If you are using Oracle databases, you cannot use the ConfigDMS utility to create the databases. You must create the databases using the database creation scripts provided with the product before running the utility.

For information about the procedures for creating these databases before running the utility, see "Creating the SOA Domain Management Server database" on page 184.

Installation tasks

You can use the utility to complete any of the following installation tasks:

- If you are performing a fresh installation of ITCAM for SOA version 7.2 fix pack 1, use the SOA Domain Management Server Configuration utility to configure SOA Domain Management Server and optionally configure Tivoli Common Object Repository.
- If you configured SOA Domain Management Server for ITCAM for SOA version 7.2 fix pack 1 but not Tivoli Common Object Repository, you can use the SOA Domain Management Server Configuration utility to configure Tivoli Common Object Repository at a later point.

Upgrade and update tasks

You can use the utility to complete any of the following upgrade and update tasks:

- If you are upgrading from ITCAM for SOA version 7.1.1, you use the SOA Domain Management Server Configuration utility to upgrade SOA Domain Management Server and Tivoli Common Object Repository (if it is configured).
- When you are updating from ITCAM for SOA version 7.2 to version 7.2 fix pack 1, use the SOA Domain Management Server Configuration utility to update SOA Domain Management Server and Tivoli Common Object Repository (if it is configured).
- If you are upgrading or updating a remote SOA Domain Management Server Configuration utility database, you must also run a migration script to migrate the database. For more information, see “Upgrading or updating a previous topology configured remotely” on page 205.

Remember: When you are upgrading from ITCAM for SOA version 7.1.1, you must upgrade topology support to version 7.2 before you update topology support to 7.2 fix pack 1.

Authentication tasks

You can use the utility to perform any of the following authentication tasks:

- If your SOA Domain Management Server database password changed, you use the SOA Domain Management Server Configuration utility to update the database password used to access the SOA Domain Management Server database. The password cannot contain the ’$’ symbol.
- If your Tivoli Common Object Repository database password changed, you use the SOA Domain Management Server Configuration utility to update the database password used to access the Tivoli Common Object Repository database.

Upgrading from a previous version

You must upgrade from ITCAM for SOA version 7.1.1 (all releases) to ITCAM for SOA version 7.2 before you update the agent to ITCAM for SOA version 7.2 Fix Pack 1.

Upgrading from Version 7.1.1 (all releases)

When you upgrade from a previous ITCAM for SOA version 7.1.1 (all releases) installation to a 7.2 installation, you run the SOA Domain Management Server Configuration utility (`ConfigDMS`) to upgrade the configuration for SOA Domain Management Server, and optionally, for Tivoli Common Object Repository, if it exists. In version 7.1.1 (all releases), the Tivoli Common Object Repository component is optional. The `ConfigDMS` utility automatically detects whether Tivoli Common Object Repository is configured, and performs the upgrade.

Important: Before upgrading to ITCAM for SOA version 7.2, you must verify that the databases you use for SOA Domain Management Server or Tivoli Common Object Repository are at one of the minimum supported levels. For information about the supported versions of the databases, see the prerequisites for ITCAM for SOA from the Software product compatibility reports website. For more information about accessing these reports, see “Required software” on page 15.

Upgrading SOA Domain Management Server

The `ConfigDMS` utility automatically upgrades the SOA Domain Management Server component. If your SOA Domain Management Server version 7.1.1 database resides on a remote system, you must use the `ConfigDMS` utility with the argument `-remoteSDMS` to upgrade ITCAM for SOA support for the databases to version 7.2

and manually migrate the SOA Domain Management Server database schema on the remote system to version 7.2.

Upgrading Tivoli Common Object Repository

The SOA Domain Management Server Configuration utility automatically upgrades the Tivoli Common Object Repository component to the version 7.2 level if it is configured. User credentials and properties are preserved during the upgrade. You can upgrade from ITCAM for SOA version 7.1.1 (all releases) to ITCAM for SOA version 7.2. If your Tivoli Common Object Repository version 7.1.1 database resides on a remote system, you must use the `ConfigDMS` utility with the argument `-remoteTCORE` to upgrade ITCAM for SOA support for the databases to version 7.2.

When you upgrade both SOA Domain Management Server and Tivoli Common Object Repository from a previous ITCAM for SOA version 7.1.1 (all releases) configuration to a version 7.2 configuration, SOA Domain Management Server is upgraded first, and then the upgrade of Tivoli Common Object Repository occurs automatically (you are not first prompted to continue with the upgrade of Tivoli Common Object Repository). If either part of this upgrade process does not complete successfully, an error message is displayed. You must resolve the problem and then run the `ConfigDMS` utility again.

Updating from ITCAM for SOA V7.2 to version V7.2 Fix Pack 1

When you update topology support from ITCAM for SOA 7.2 to ITCAM for SOA version 7.2 Fix Pack 1, the procedure to follow is the same as the procedure for upgrading from ITCAM for SOA 7.1.1 (all releases) to ITCAM for SOA version 7.2.

To update topology support from ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1, run the `ConfigDMS` utility to update the configuration for SOA Domain Management Server, and optionally, for Tivoli Common Object Repository, if it exists. The `ConfigDMS` utility automatically detects whether Tivoli Common Object Repository is configured, and performs the update.

Updating SOA Domain Management Server

The `ConfigDMS` utility automatically updates the SOA Domain Management Server component. If your SOA Domain Management Server version 7.2 database resides on a remote system, you must use the `ConfigDMS` utility with the argument `-remoteSDMS` to perform the following activities:

- Update ITCAM for SOA support for the databases to version 7.2 Fix Pack 1
- Migrate the SOA Domain Management Server database schema on the remote system to version 7.2.

Updating Tivoli Common Object Repository

The `ConfigDMS` utility automatically updates the Tivoli Common Object Repository component to the version 7.2 Fix Pack 1 level if it is configured. User credentials and properties are preserved during the update.

If your Tivoli Common Object Repository version 7.2 database resides on a remote system, you must use the `ConfigDMS` utility with the argument `-remoteTCORE` to update ITCAM for SOA support for the databases to version 7.2 Fix Pack 1.

When you update both SOA Domain Management Server and Tivoli Common Object Repository from aITCAM for SOA version 7.2 configuration to a version 7.2 Fix Pack 1 configuration, SOA Domain Management Server is updated first, and then the update of Tivoli Common Object Repository occurs automatically. If either part of this update process does not complete successfully, an error message is displayed. You must resolve the problem and then run the `ConfigDMS` utility again.

Upgrading and updating in silent mode

The *upgrade* property in the silent configuration file specifies whether to upgrade or update a previous configuration of both SOA Domain Management Server and Tivoli Common Object Repository, depending on already configured components:

- If only SOA Domain Management Server version 7.1.1 is configured, SOA Domain Management Server is upgraded to version 7.2.
- If SOA Domain Management Server and Tivoli Common Object Repository version 7.1.1 is configured, both are upgraded to version 7.2.
- If only SOA Domain Management Server version 7.2 is configured, SOA Domain Management Server is upgraded to version 7.2 Fix Pack 1.
- If SOA Domain Management Server and Tivoli Common Object Repository version 7.2 is configured, both are upgraded to version 7.2 Fix Pack 1.

For information about the silent response file properties that you must specify while upgrading in silent mode, see "Running the `ConfigDMS` utility in silent mode" on page 219.

Launching the `ConfigDMS` utility

To run the `ConfigDMS` utility, complete the following steps on the local Linux or UNIX computer system where Tivoli Enterprise Portal Server is installed:

1. Verify that you are logged in with a user that has the appropriate permissions as described in "Database and User Permissions" on page 178.
2. If you are running the `ConfigDMS` utility in graphical user interface mode on Linux or UNIX operating systems, verify that you can run X Window System-based applications to ensure that you have appropriate permissions.
3. Complete these steps to source the DB2 instance profile if one of the following conditions applies:
   - You are using the `ConfigDMS` to configure the SOA Domain Management Server or Tivoli Common Object Repository for the first time and the utility is being used to create a local DB2 database.
   - You are using the `ConfigDMS` utility to upgrade from ITCAM for SOA V7.1.1 to 7.2. The SOA Domain Management Server is using a local DB2 database in this case.
   - You are using the `ConfigDMS` utility to update from ITCAM for SOA V7.2 to 7.2 Fix Pack 1. The SOA Domain Management Server is using a local DB2 database in this case.

   a. Navigate to /*home*/*dbuser*/sqllib, where *dbuser* is the DB2 instance user name (for example, db2inst1).

   b. Run the following command:

   ```
   . ./db2profile
   ```

   Tip: Be sure to leave a space between the first period and the **`./db2profile`** command
4. Complete the following steps to set environment variables for *ORACLE_SID*, *ORACLE_HOME* and *PATH*, and to source the Oracle `oraenv` file if you are using the `ConfigDMS` utility to upgrade from ITCAM for SOA version 7.1.1 to version 7.2 or update from ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1 and the SOA Domain Management Server is using a local Oracle database:

a. Set the *ORACLE_SID* environment variable to the name of the SOA Domain Management Server database. For example, export ORACLE_SID=KD4SDMS

   Important: On a computer system that has multiple installations of ITCAM for SOA, ensure that the database name specified in ORACLE_SID is the name of the database that is being upgraded.

b. Set the *ORACLE_HOME* environment variable to the directory where the Oracle database server is installed. For example, export ORACLE_HOME=/app/oracle/product/10.2.0/db_1

c. Set the PATH environment variable to the directory where the sqlplus utility is located. For example, export PATH=$PATH:$ORACLE_HOME/bin

d. Navigate to the /usr/local/bin directory.

e. Run the following command to source the Oracle oraenv file:

```
. ./oraenv
```

   Tip: Be sure to leave a space between the first period and the **./oraenv** command

5. Depending on your intended task, you must run the ConfigDMS utility from one of two possible locations:
   - Navigate to the *ITM_Home*/*Platform*/cq/Products/KD4/latest/bin directory if any of the following conditions apply:
     – You are initially running the SOA Domain Management Server Configuration utility to configure SOA Domain Management Server or Tivoli Common Object Repository for the first time.
     – You are running the SOA Domain Management Server Configuration utility to *upgrade* or *update* from a previous configuration.
   - Navigate to the *ITM_Home*/*Platform*/cq/Products/KD4/bin directory if the following conditions apply:
     – You configured or upgraded SOA Domain Management Server and Tivoli Common Object Repository previously to the version 7.2 Fix Pack 1 level.
     – You are now running the ConfigDMS utility again to *update the authentication* to access SOA Domain Management Server or Tivoli Common Object Repository databases.
6. Run the **ConfigDMS.sh** script. This script provides several command options, described by the following syntax:

```
ConfigDMS.sh [-console | -silent {silent_file}] [-debug {debug_file}]
[-remoteSDMS] [-remoteTCORE]
```

   Important: When you are installing ITCAM for SOA, do not run the ConfigDMS utility as the DB2 administrator user.

These command options are described further in “ConfigDMS command options”

ConfigDMS command options

Running the ConfigDMS utility with no command options starts the ConfigDMS utility in the default graphical user interface mode. This configuration utility prompts you for the necessary parameters to create databases and configure the SOA Domain Management Server and optional Tivoli Common Object Repository support. For more information about running ConfigDMS, see “Running the ConfigDMS utility in Graphical User Interface mode” on page 200.

The command options for the ConfigDMS utility are as follows:

–console

This option runs the ConfigDMS utility in command-line mode, if you prefer to use that over the Install Shield graphical user interface. This option cannot be specified together with the –silent option. For more information, see "Running the ConfigDMS utility in console mode" on page 218.

Examples:

```
./ConfigDMS.sh -console
```

–silent [*dir_path*/]*silent_file*

This option runs the ConfigDMS utility in silent mode. The *silent_file* file is a simple properties file that you create, containing the necessary parameters to create databases and configure the SOA Domain Management Server and optional Tivoli Common Object Repository support. If this file is not stored in the same directory path where you run the ConfigDMS utility (either the *ITM_Home*/CNPS/Products/KD4/latest/bin directory or the *ITM_Home*/CNPS/Products/KD4/bin directory, specify the fully qualified directory path where this file is located. (For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.) This option cannot be specified together with the –console option. For more information, see "Running the ConfigDMS utility in silent mode" on page 219.

Examples:

```
./ConfigDMS.sh -silent config.properties
```

–debug [*dir_path*/]*debug_file*

This option can be specified alone or after specifying either the –console or –silent options. The ConfigDMS utility is run in either graphical user interface mode, console mode, or silent mode, and log information is written to the *debug_file* file for later examination and diagnosis of problems by IBM Software Support.

The debug log file is a plain text file stored in a specified directory path, or, if no directory path is specified, in the same directory where you run the ConfigDMS utility (either *ITM_Home*/CNPS/Products/KD4/latest/bin or *ITM_Home*/CNPS/Products/KD4/bin).

If you do not specify a file name for *debug_file*, the utility is not started, and you are presented with the syntax information as a reminder.

Examples:

```
./ConfigDMS.sh -console -debug debuglog
```

-remoteSDMS

This option can be specified alone or together with the -remoteTCORE option. The -remoteSDMS option can be specified after the –debug option, or after specifying either the –console or –silent options. The -remoteSDMS option prevents the SQL migrate scripts for the SOA Domain Management Server from running locally. The -remoteSDMS option must be specified when upgrading or updating a remote SOA Domain Management Server database.

-remoteTCORE

This option can be specified alone or together with the -remoteSDMS option. The -remoteTCORE option can be specified after the –debug option, or after specifying either the –console or –silent options. The -remoteTCORE option prevents the SQL migrate scripts for Tivoli Common Object Repository from running locally. The `-remoteTCORE` option must be specified when upgrading or updating a remote Tivoli Common Object Repository database.

Logging information

Logging information is written to a log file in the *ITM_Home*/`logs` directory, named in this format: kd4_sdms_config*date_timestamp*.log. (For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.) Scroll to the end of this log file for the most recent information. See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for assistance with problems you might encounter while configuring support for SOA Domain Management Server and Tivoli Common Object Repository.

If errors are encountered during configuration, messages are displayed with information to assist you in determining the problem.

For more information about typical errors you might encounter and for a complete description of error messages and possible recovery options, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*

Running the `ConfigDMS` utility in Graphical User Interface mode

Running the `ConfigDMS` utility from an ITCAM for SOA version 7.2 or an ITCAM for SOA version 7.2 Fix Pack 1 installation without specifying either the `–console` or `–silent` options starts the `ConfigDMS` utility in graphical user interface mode.

Running the `ConfigDMS` utility from an ITCAM for SOA V7.2 installation

After you select the preferred language, a welcome page is presented with some brief information about the `ConfigDMS` utility. After you click **Next**, the `ConfigDMS` utility detects one of the following conditions:

SOA Domain Management Server or Tivoli Common Object Repository support is configured for ITCAM for SOA V7.2

In this case, the utility informs you that the application will be upgraded to the current version. See “Upgrading a version 7.1.1 topology configured locally” on page 202 for the procedure.

Important: If you are upgrading a database from version 7.1.1 (all versions) and the database is located remotely, you must use the *-remoteSDMS* or *-remoteTCORE* arguments to launch the `ConfigDMS` utility.

ITCAM for SOA support for SOA Domain Management Server and Tivoli Common Object Repository is not yet configured

In this case, the utility offers you choices to configure SOA Domain Management Server and, optionally, Tivoli Common Object Repository at the version 7.2 level. See “Configuring topology support for the first time” on page 208 for the procedure.

ITCAM for SOA V7.2 support for the SOA Domain Management Server is configured but not for Tivoli Common Object Repository

The utility offers you one or more of the following configuration choices:

- If your SOA Domain Management Server database password has changed recently, you can update the authentication in your current SOA Domain Management Server configuration. For the procedure, see “Updating authentication for SOA Domain Management Server” on page 217.

- You can configure the optional support for Tivoli Common Object Repository. For the procedure, see "Configuring the Tivoli Common Object Repository" on page 213.

ITCAM for SOA V7.2 support for the SOA Domain Management Server and Tivoli Common Object Repository are both configured

In this case, the utility offers you the following configuration choices:

- If your SOA Domain Management Server database password has changed recently, you can update the authentication in your current SOA Domain Management Server configuration. For the procedure, see "Updating authentication for SOA Domain Management Server" on page 217.
- If your Tivoli Common Object Repository database password has changed recently, you can update the authentication in your current Tivoli Common Object Repository configuration. For the procedure, see "Updating authentication for Tivoli Common Object Repository" on page 218.

Running the `ConfigDMS` utility from an ITCAM for SOA V7.2 Fix Pack 1 installation

After you select the preferred language, a welcome page is presented with some brief information about the `ConfigDMS` utility. After you click **Next**, the `ConfigDMS` utility detects one of the following conditions:

SOA Domain Management Server or Tivoli Common Object Repository support is configured for ITCAM for SOA V7.2 Fix Pack 1

In this case, the utility informs you that the application will be updated to the current version. See "Updating a version 7.2 topology configured locally" on page 204 for the procedure.

Important: If you are updating a database from version 7.2 and the database is located remotely, you must use the *-remoteSDMS* or *-remoteTCORE* arguments to start the `ConfigDMS` utility.

ITCAM for SOA support for SOA Domain Management Server and Tivoli Common Object Repository is not yet configured

In this case, the utility offers you choices to configure SOA Domain Management Server and, optionally, Tivoli Common Object Repository at the version 7.2 Fix Pack 1 level. See "Configuring topology support for the first time" on page 208 for the procedure.

ITCAM for SOA V7.2 Fix Pack 1 support for the SOA Domain Management Server is configured but not for Tivoli Common Object Repository

The utility offers you one or more of the following configuration choices:

- If your SOA Domain Management Server database password has changed recently, you can update the authentication in your current SOA Domain Management Server configuration. For the procedure, see "Updating authentication for SOA Domain Management Server" on page 217.
- You can configure the optional support for Tivoli Common Object Repository. For the procedure, see "Configuring the Tivoli Common Object Repository" on page 213.

ITCAM for SOA V7.2 Fix Pack 1 support for the SOA Domain Management Server and Tivoli Common Object Repository are both configured

In this case, the utility offers you the following configuration choices:

- If your SOA Domain Management Server database password has changed recently, you can update the authentication in your current SOA Domain Management Server configuration. For the procedure, see "Updating authentication for SOA Domain Management Server" on page 217.
- If your Tivoli Common Object Repository database password has changed recently, you can update the authentication in your current Tivoli Common Object Repository configuration. For the procedure, see "Updating authentication for Tivoli Common Object Repository" on page 218.

Upgrading topology support using the ConfigDMS utility

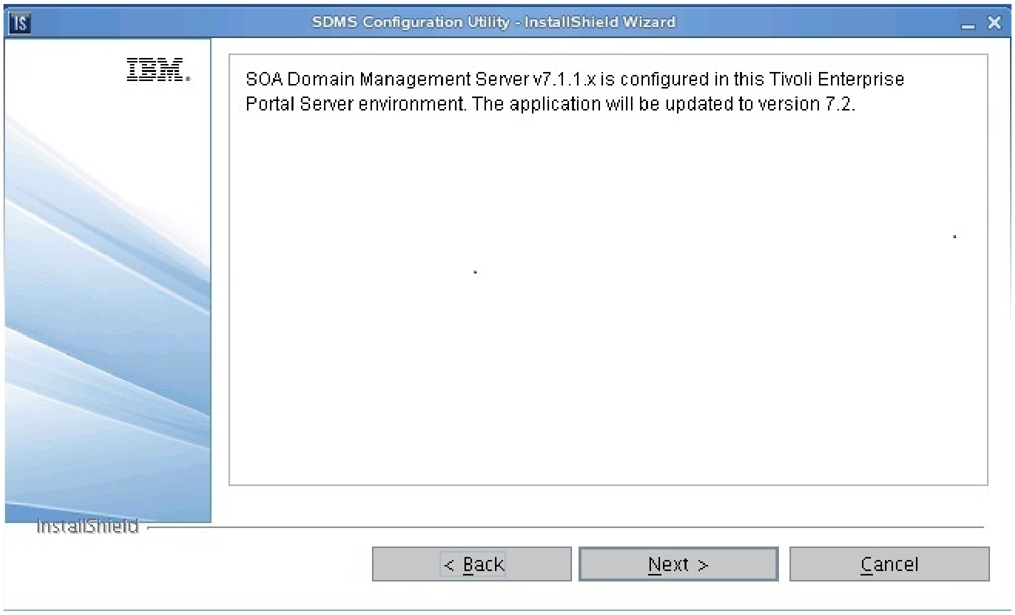
You can upgrade topology support from ITCAM for SOA version 7.1.1 to version 7.2. When you have configured topology support for ITCAM for SOA version 7.2, you must update topology to ITCAM for SOA version 7.2 Fix Pack 1.

Upgrading a version 7.1.1 topology configured locally: If you already have a configuration of SOA Domain Management Server and Tivoli Common Object Repository support from a previous version of ITCAM for SOA in your local Tivoli Enterprise Portal Server environment, the `ConfigDMS` utility upgrades this support to ITCAM for SOA version 7.2. When upgrading from ITCAM for SOA version 7.1.1 (all releases) to version 7.2, the utility does not prompt you for upgrade information.

Important: The process might take some time to complete as the database is upgraded, depending on its size. It can take 15 minutes or longer, so do not stop the `ConfigDMS` utility in the middle of an upgrade.

To upgrade a topology, complete the following steps:

1. Start the ConfigDMS utility in graphical user interface mode. For more information, see "Running the `ConfigDMS` utility in Graphical User Interface mode" on page 200.
2. The utility informs you that the application will be updated to the current version.

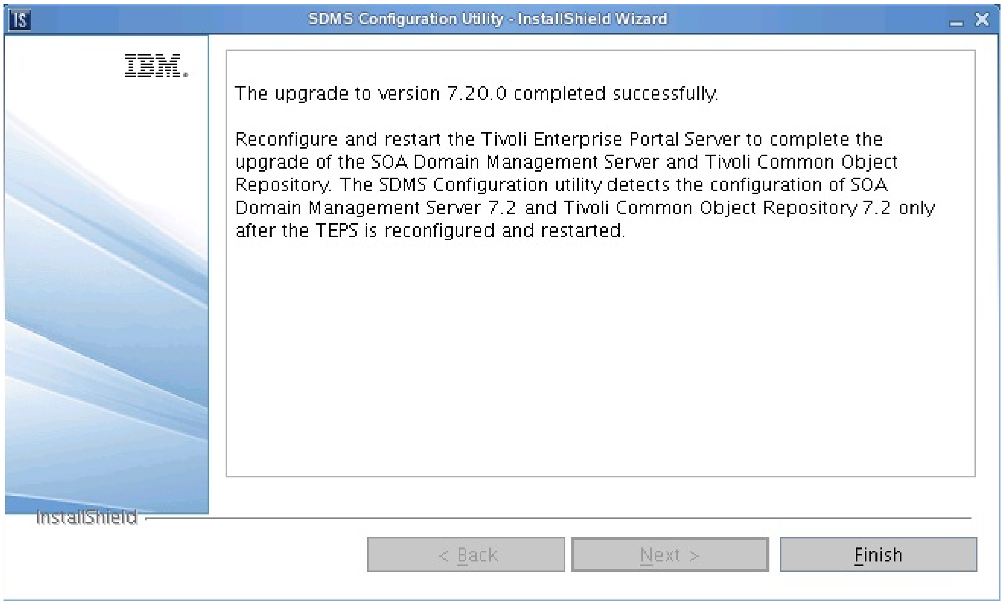


SOA Domain Management Server v7.1.1.x is configured in this Tivoli Enterprise Portal Server environment. The application will be updated to version 7.2.

Figure 37. Message indicating that the application will be updated to the current version

Click **Next**.

3. The utility upgrades Tivoli Common Object Repository support to the current version. If there are errors, you are notified and the only option is to exit the utility. If you experience errors while upgrading your SOA Domain Management Server or Tivoli Common Object Repository support, consult with your local database administrator for assistance or contact IBM Software Support.
4. The utility notifies you that the upgrade has completed.



The upgrade to version 7.20.0 completed successfully.

Reconfigure and restart the Tivoli Enterprise Portal Server to complete the upgrade of the SOA Domain Management Server and Tivoli Common Object Repository. The SDMS Configuration utility detects the configuration of SOA Domain Management Server 7.2 and Tivoli Common Object Repository 7.2 only after the TEPS is reconfigured and restarted.

Figure 38. Message indicating that the upgrade is complete

5. Click **Finish** to exit the utility.

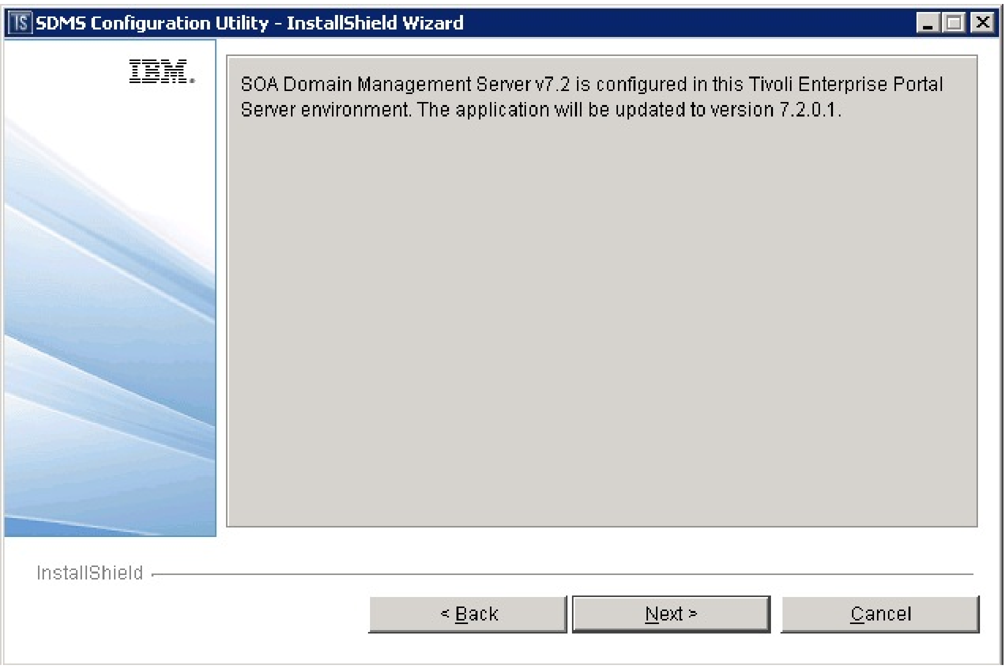
6. Rebuild and restart Tivoli Enterprise Portal Server for the upgrade to take effect. For more information about rebuilding the portal server, see "Rebuilding and restarting the Tivoli Enterprise Portal Server" on page 227.

The `collation.properties` and `bulkload.properties` files in the *ITM_Home*/*platform*/`cq/Products/KD4/tcore/etc` directory are renamed to `bulkload.properties.backup` and `collation.properties.backup1`. (For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.) If you modified any properties in a previous version of these files, you must manually merge the changes into ITCAM for SOA version 7.2 files after migration is complete.

Updating a version 7.2 topology configured locally: If you already have a configuration of SOA Domain Management Server and Tivoli Common Object Repository support from a previous version of ITCAM for SOA in your local Tivoli Enterprise Portal Server environment, the `ConfigDMS` utility updates this support to ITCAM for SOA version 7.2 Fix Pack 1. When updating from ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1, the utility does not prompt you for upgrade information.

To update a topology, complete the following steps:

1. Start the ConfigDMS utility in graphical user interface mode. For more information, see "Running the `ConfigDMS` utility in Graphical User Interface mode" on page 200.
2. The utility informs you that the application will be updated to the current version.



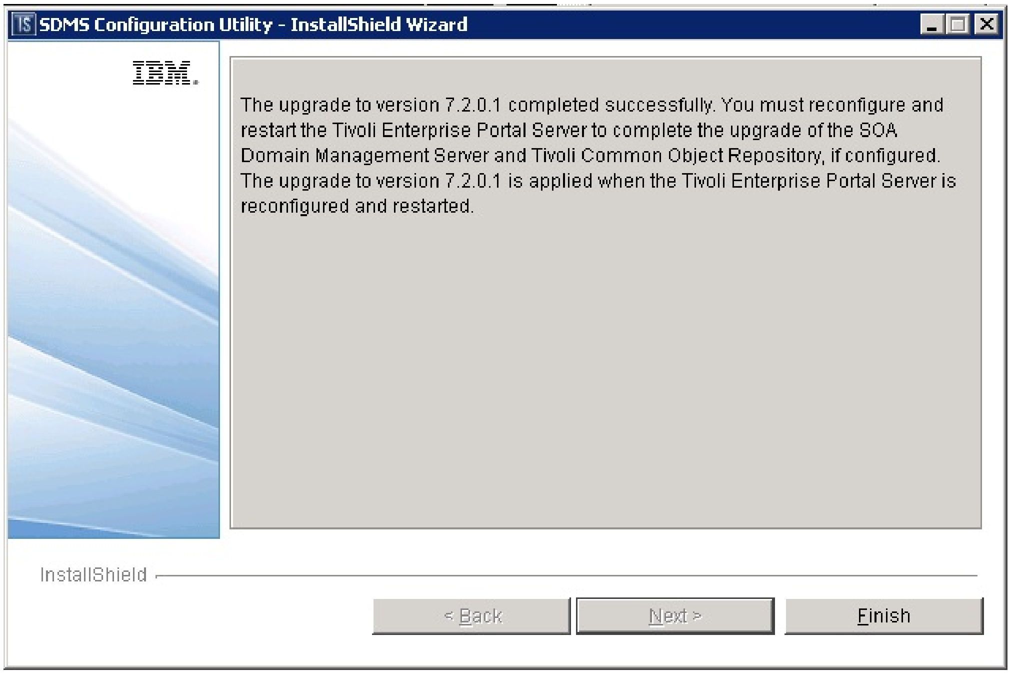
SOA Domain Management Server v7.2 is configured in this Tivoli Enterprise Portal Server environment. The application will be updated to version 7.2.0.1.

Figure 39. Message indicating that the application will be updated to the current version

   Click **Next**.
3. The utility upgrades Tivoli Common Object Repository support to the version 7.2 Fix Pack 1. If there are errors, you are notified and the only option is to exit the utility. If you experience errors while upgrading your SOA Domain

Management Server or Tivoli Common Object Repository support, consult with your local database administrator for assistance or contact IBM Software Support.

4. The utility notifies you that the update to version 7.2 Fix Pack 1 has completed.



The upgrade to version 7.2.0.1 completed successfully. You must reconfigure and restart the Tivoli Enterprise Portal Server to complete the upgrade of the SOA Domain Management Server and Tivoli Common Object Repository, if configured. The upgrade to version 7.2.0.1 is applied when the Tivoli Enterprise Portal Server is reconfigured and restarted.

Figure 40. Message indicating that the upgrade is complete

5. Click **Finish** to exit the utility.
6. Rebuild and restart Tivoli Enterprise Portal Server for the upgrade to take effect. For more information about rebuilding the portal server, see “Rebuilding and restarting the Tivoli Enterprise Portal Server” on page 227.

The `collation.properties` and `bulkload.properties` files in the *ITM_Home*/*platform*/`cq/Products/KD4/tcore/etc` directory are renamed to `bulkload.properties.backup` and `collation.properties.backup1`. (For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.) If you modified any properties in a previous version of these files, you must manually merge the changes into ITCAM for SOA version 7.2 Fix Pack 1 files after migration is complete.

Upgrading or updating a previous topology configured remotely: If you already have a configuration of SOA Domain Management Server, or SOA Domain Management Server and Tivoli Common Object Repository from a previous version of ITCAM for SOA installed on a *remote* system, you must use the `ConfigDMS` utility to complete the following:

- Upgrade support for the databases to the later version of ITCAM for SOA:
  - If you are upgrading to ITCAM for SOA version 7.2 before you update to ITCAM for SOA version 7.2 Fix Pack 1, upgrade support for the databases to version 7.2.
  - If you are updating to ITCAM for SOA version 7.2 Fix Pack 1, update support for the databases to version 7.2 Fix Pack 1.
- Manually migrate the SOA Domain Management Server database schema on the remote system to the later version

- Rebuild and restart the Tivoli Enterprise Portal Server.

To upgrade a remote DB2 or Oracle database, complete the following steps:

1. Before running the ConfigDMS utility to upgrade or update the databases in step 2, set the environment variables for the SOA Domain Management Server database if the SOA Domain Management Server database is installed locally and the Tivoli Common Object Repository database is installed remotely.

   For information about how to set the environment variables, see step "Launching the ConfigDMS utility" on page 197 for a DB2 database or step 4 on page 197 for an Oracle database in "Launching the ConfigDMS utility" on page 197.
2. On the Tivoli Enterprise Portal Server where the ITCAM for SOA agent is installed, run the ConfigDMS utility with the *-remoteSDMS* argument if the SOA Domain Management Server database is remote and the *-remoteTCORE* argument if the Tivoli Common Object Repository database is remote. For example:

   ```
   TEPS_Home/platform/cq/Products/KD4/latest/bin/ConfigDMS.sh tcore/etc
   -remoteSDMS -remoteTCORE
   ```

   The -remoteSDMS and the -remoteTCORE arguments can be specified with either the -console or -silent arguments.

   If there are errors, you are notified and the only option is to exit the utility. If you experience errors while upgrading your SOA Domain Management Server or Tivoli Common Object Repository support, consult with your local database administrator for assistance or contact IBM Software Support. You are notified when the upgrade completes successfully, and can exit the utility.
3. If the SOA Domain Management Server database is on a remote system, perform the following steps to migrate the database:
   a. Copy the kd4RemoteDB.tar.gz file from *TEPS_home*/*platform*/cq/Products/KD4/latest/bin/ to the remote database host.
   b. Verify that the databases and any required services are running on the remote host.
   c. Source the db2profile if you are using a DB2 database or source the oraenv file if you are using an Oracle database.

      For more information about sourcing the db2profile, see step 3 on page 197 of "Launching the ConfigDMS utility" on page 197.

      For more information about sourcing the oraenv, see step 4 on page 197 of "Launching the ConfigDMS utility" on page 197.
   d. If you are upgrading from ITCAM for SOA version 7.1.1 to version 7.2, locate the script to migrate the database schema from ITCAM for SOA version 7.1.1 on the remote system:
      - If the remote database is a DB2 database, run the following command as an administrator:

        ```
        kd4MigrateDB2db.sh sdms_db2_7113_to_72.sql DBNAME
        ```

        where *DBNAME* is the name of the SOA Domain Management Server database.
      - If the remote database is an Oracle database, run the following command as an administrator:

        ```
         kd4MigrateOracledb.sh sdms_oracle_7113_to_72.sql DBNAME SDMS
        [DBUSER PASSWD]
        ```

        Where:

DBNAME
Name of the SOA Domain Management Server database. The name is the Oracle System Identifier of the database.

DBUSER
Name of the SOA Domain Management Server database user.

PASSWD
Password associated with *DBNAME*.

Important: The process might take some time to complete as the database is upgraded, depending on its size. It can take 15 minutes or longer. Do not stop the `kd4MigrateDB2db.sh` or the `kd4MigrateOracledb.sh` migrate script in the middle of an upgrade.

e. If you are updating from ITCAM for SOA version 7.2 to version 7.2 Fix Pack 1, locate the script to migrate the database schema from ITCAM for SOA version 7.2 on the remote system.
   - If the remote database is a DB2 database, run the following command as an administrator:

     ```
     kd4MigrateDB2db.sh sdms_db2_72_to_7201.sql DBNAME
     ```

     where *DBNAME* is the name of the SOA Domain Management Server database.
   - If the remote database is an Oracle database, run the following command as an administrator:

     ```
      kd4MigrateOracledb.sh sdms_oracle_72_to_7201.sql DBNAME SDMS
     [DBUSER PASSWD]
     ```

     Where:

     DBNAME
     Name of the SOA Domain Management Server database. The name is the Oracle System Identifier of the database.

     DBUSER
     Name of the SOA Domain Management Server database user.

     PASSWD
     Password associated with *DBNAME*.

4. Rebuild and restart the Tivoli Enterprise Portal Server for the upgrade to take effect. For more information about rebuilding the portal server, see “Rebuilding and restarting the Tivoli Enterprise Portal Server” on page 227.

Properties files renamed

The `collation.properties` and `bulkload.properties` files in the *`ITM_Home`*/*`Platform`*/`cq/Products/KD4/tcore/etc` directory are renamed to `bulkload.properties.backup` and `collation.properties.backup1`. (For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.) If you modified any properties in a previous version of these files, you must manually merge the changes into the latest version of ITCAM for SOA after migration is complete.

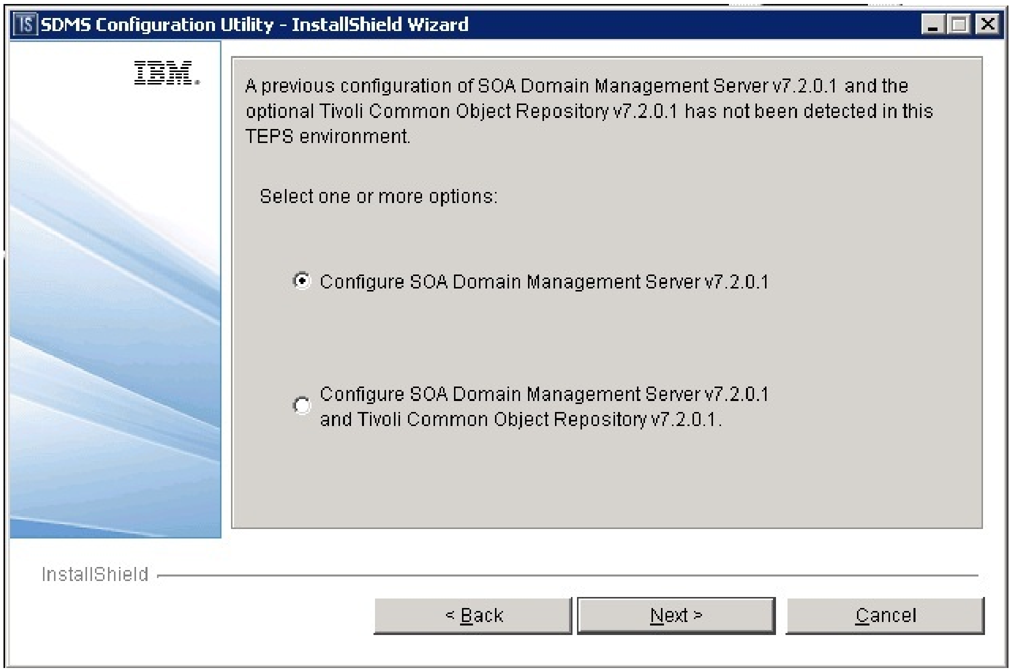
Configuring topology support using the ConfigDMS utility

If you do not have a previous installation of ITCAM for SOA, you can configure topology support for ITCAM for SOA version 7.2 Fix Pack 1 without first configuring topology support for ITCAM for SOA version 7.2.

Configuring topology support for the first time: If you do not have a previous configuration of SOA Domain Management Server topology support in your portal server environment, then the `ConfigDMS` utility configures this support for you.

You are asked to select one of the following options:

- Configure support for SOA Domain Management Server only.
- Configure support for both SOA Domain Management Server and Tivoli Common Object Repository.



SDMS Configuration Utility - InstallShield Wizard

A previous configuration of SOA Domain Management Server v7.2.0.1 and the optional Tivoli Common Object Repository v7.2.0.1 has not been detected in this TEPS environment.

Select one or more options:

● Configure SOA Domain Management Server v7.2.0.1

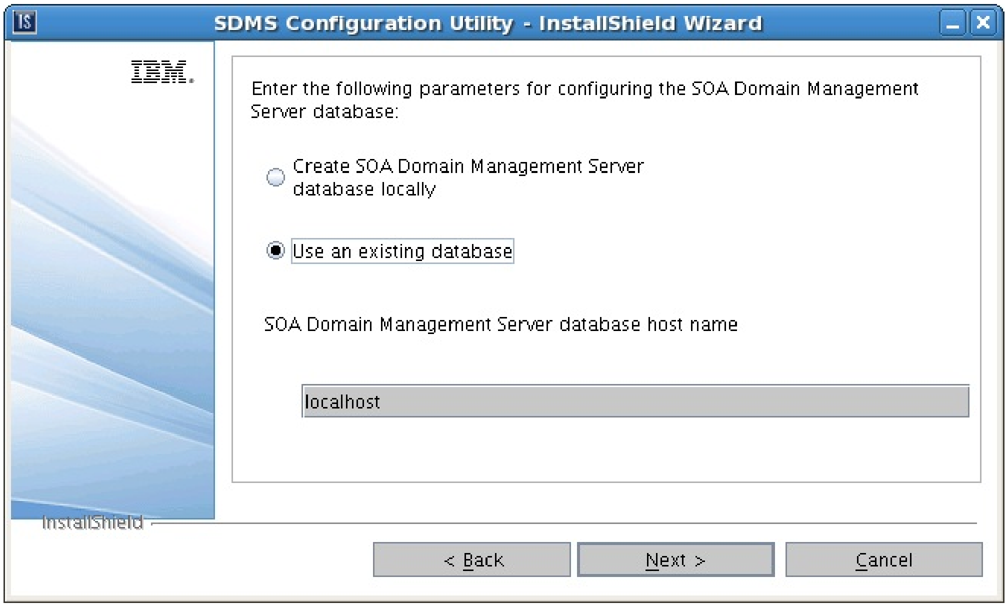
○ Configure SOA Domain Management Server v7.2.0.1 and Tivoli Common Object Repository v7.2.0.1.

Figure 41. Options for configuring topology support

For the procedures, see “Configuring the SOA Domain Management Server” and “Configuring the Tivoli Common Object Repository” on page 213.

Configuring the SOA Domain Management Server: To configure SOA Domain Management Server, complete the following steps:

1. Start the `ConfigDMS` utility in graphical user interface mode. For more information, see “Running the `ConfigDMS` utility in Graphical User Interface mode” on page 200.
2. Specify whether to create the SOA Domain Management Server database locally, or whether to use an existing (local or remote) database that you have previously created.



Enter the following parameters for configuring the SOA Domain Management Server database:

○ Create SOA Domain Management Server database locally

● Use an existing database

SOA Domain Management Server database host name

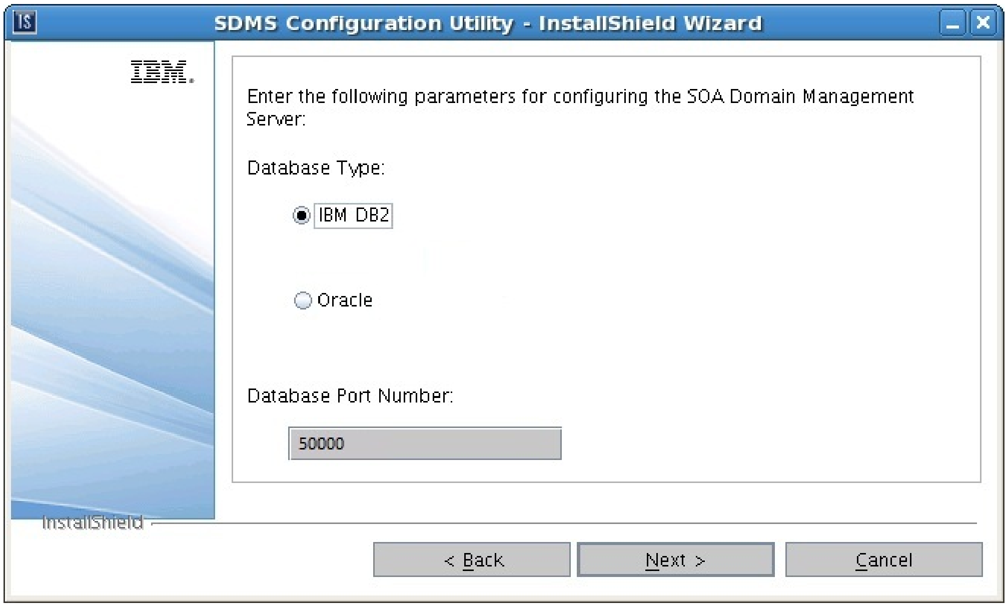
localhost

Figure 42. Specifying to create the SOA Domain Management Server database or use an existing database

If you prefer to use an existing local or remote database, select **Use an existing database** and enter the hostname of the computer where the SOA Domain Management Server database is located. You can also specify *localhost* to use an existing local database.

Important: If you plan to use an Oracle database to support the SOA Domain Management Server, you must use an existing database that is either on the local portal server or is on a remote database server. You must also use an Oracle database for the Tivoli Common Object Repository. For information about using script files to manually create the local or remote SOA Domain Management Server database before running the `ConfigDMS` utility, see "Creating the SOA Domain Management Server database" on page 184.

3. Select the database type.



Enter the following parameters for configuring the SOA Domain Management Server:

Database Type:

● IBM DB2

○ Oracle

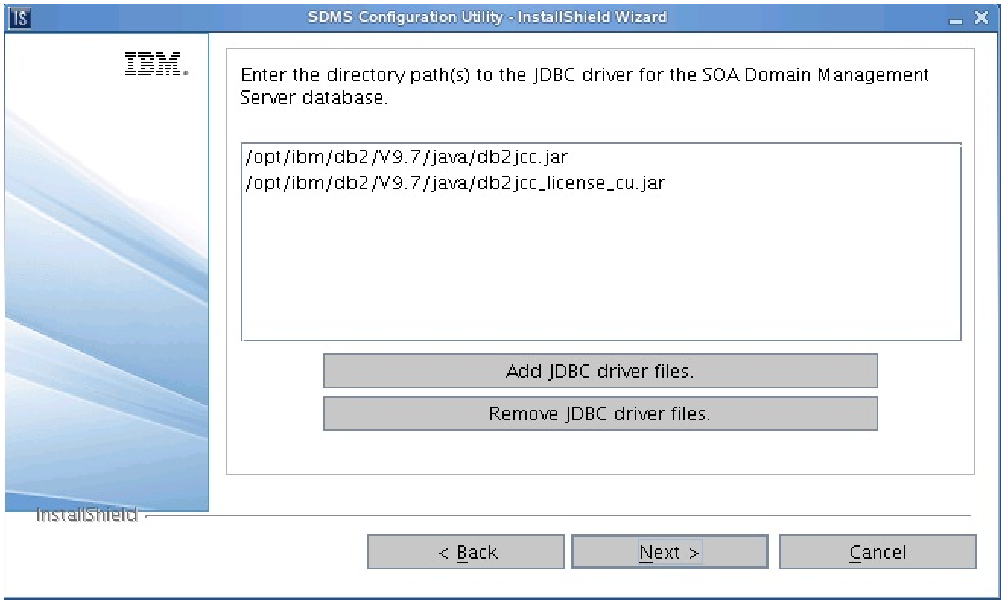
Database Port Number:

50000

Figure 43. Configuring the SOA Domain Management Server

The two possible database types are DB2 and Oracle. This parameter is automatically obtained from the Tivoli Enterprise Portal Server configuration, and the default value for this parameter is set to the current database type.

4. If you selected DB2 as the database type, complete the following steps
   a. Enter the database port number. The default port number is `50000`.
   b. Specify the fully qualified directory path to the JDBC driver class files.



SDMS Configuration Utility - InstallShield Wizard
IBM.
Add JDBC driver files.
Remove JDBC driver files.
InstallShield
< Back
Next >
Cancel

Enter the directory path(s) to the JDBC driver for the SOA Domain Management Server database.

```
/opt/ibm/db2/V9.7/java/db2jcc.jar
/opt/ibm/db2/V9.7/java/db2jcc_license_cu.jar
```

Figure 44. Specifying the JDBC drivers

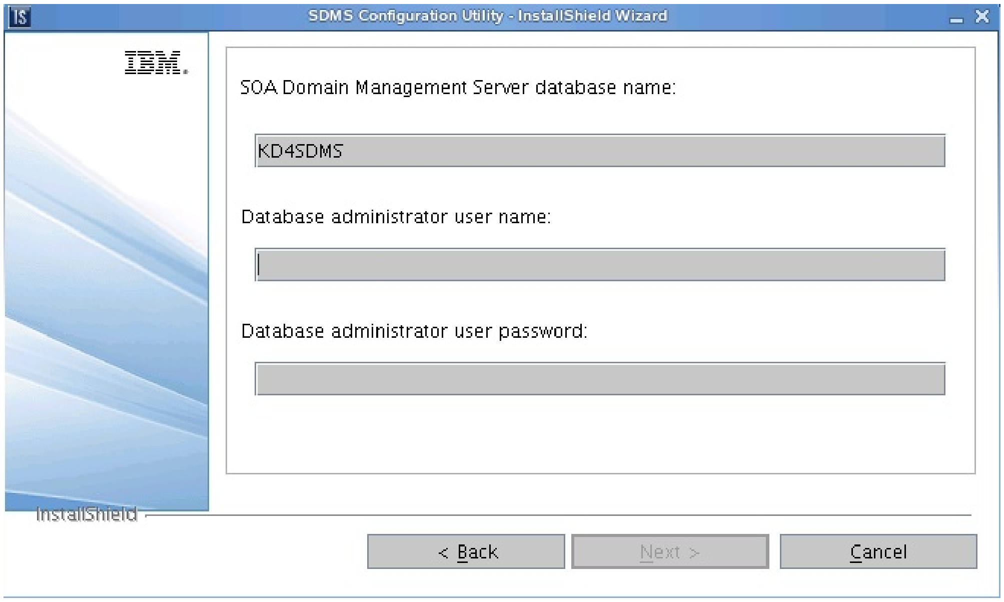
The utility searches for the driver files based on where your database application is installed, and presents these files as defaults. You can accept these defaults or specify others as needed.

The following files are the specific files that the utility searches for:

```
Instance_Owner_Home_Directory/sqllib/java/db2jcc.jar
Instance_Owner_Home_Directory/sqllib/java/db2jcc_license_cu.jar
```

The *Instance_Owner_Home_Directory* path is typically/`home/db2inst1`. The *`Instance_Owner_Home_Directory`*`/sqllib/java` path is a symbolic link to the Java directory for your DB2 installation (for example, `/opt/ibm/db2/V9.5/java` when DB2 9.5 is installed).

c. Enter the name of the SOA Domain Management Server database.



SOA Domain Management Server database name:

KD4SDMS

Database administrator user name:

Database administrator user password:

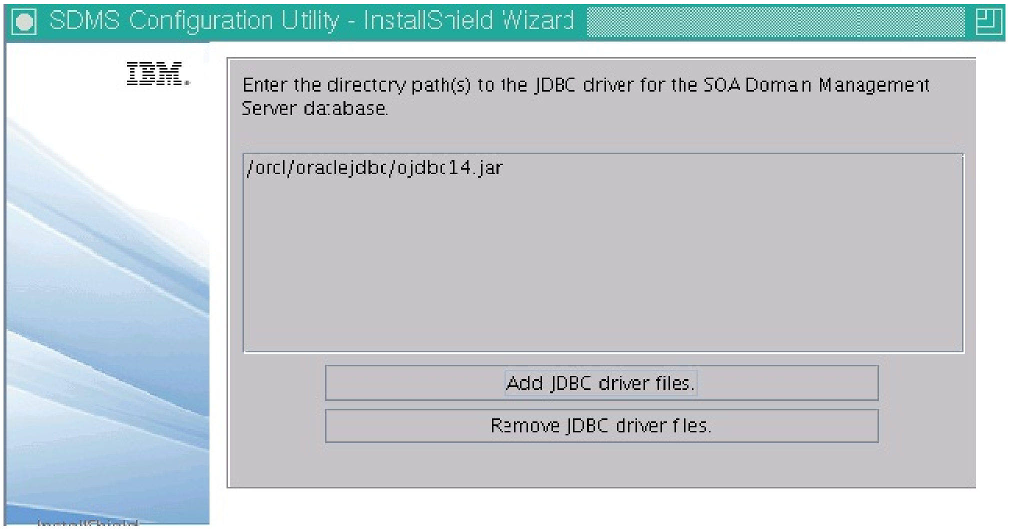
Figure 45. Specifying the SOA Domain Management Server database name and database user

The default name is `KD4SDMS` and has a limit of 8 characters.

Remember: If you specified to create the SOA Domain Management Server database locally and this database name exists on the local system, it is dropped and re-created. If you want the configuration utility to create this database for you and you do not want to drop an existing database, specify a different name.

d. Enter the database administrative user name and password (for example, the default user name and password, `db2inst1`). This user name must exist, and the configuration utility validates the specified password before continuing. The password cannot contain the '$' symbol. For more information about the authorization required for this database user, see "Database and User Permissions" on page 178.

5. If you selected Oracle as the database type, complete the following steps:
   a. Enter the fully qualified host name of the Oracle database server.
   b. Enter the database port number. The default port number is `1521`.
   c. Enter the fully qualified directory path to the Oracle JDBC driver. For example, `opt/app/ojdbc6.jar`


SDMS Configuration Utility - InstallShield Wizard
IBM.
Add JDBC driver files.
Remove JDBC driver files.
InstallShield

Enter the directory path(s) to the JDBC driver for the SOA Domain Management Server database.

/orcl/oraclejdbc/ojdbc14.jar

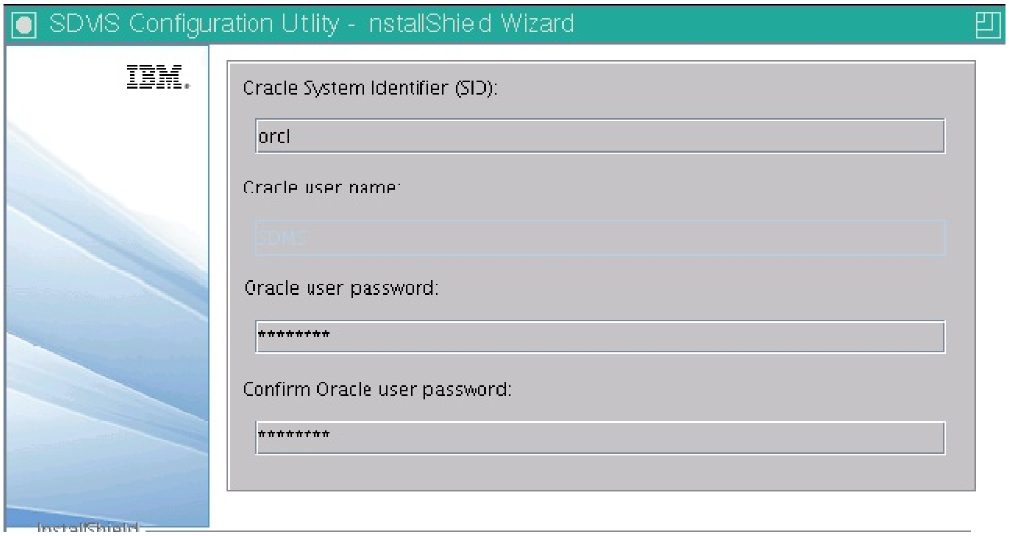
Figure 46. Specifying the JDBC drivers

These JDBC drivers are needed on the computer where the portal server is installed (where SOA Domain Management Server support is being configured).

Restriction: The `ojdbc6.jar` JDBC driver must be used with Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2. For more information about this restriction, see technote.
If you installed Oracle 10g Release 2, you must download the `ojdbc6.jar` driver from the Oracle website because it is not provided with Oracle 10g Release 2.

d. Enter the Oracle system identifier. Set the Oracle system identifier to the system identifier specified when you ran the `KD4InitOracleDB` script.

e. Enter Oracle user password. Set it to the user password specified when you ran the `kd4InitOracleDb` script.



Oracle System Identifier (SID):

orcl

Oracle user name:

SDMS

Oracle user password:

****

Confirm Oracle user password:

****

Figure 47. Specifying the SOA Domain Management Server Oracle System Identifier

f. The utility validates the specified user name and password and attempts to configure the SOA Domain Management Server. If there are errors, you are notified and can go back and correct any specified parameters, or you can exit the configuration utility.

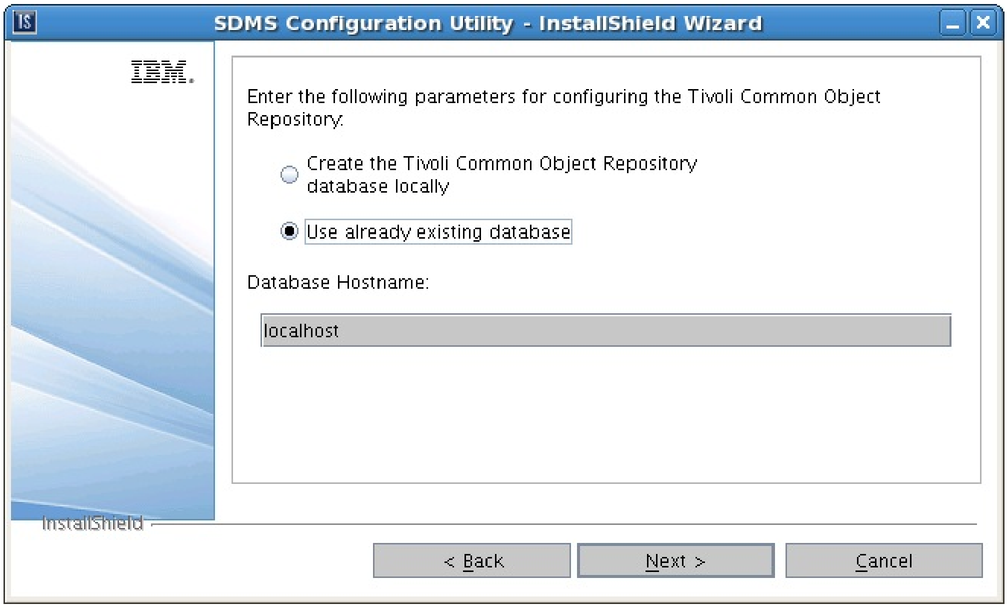
   When the configuration completes successfully, you are notified. If you selected to configure only the SOA Domain Management Server, you can exit the configuration utility. If you selected to configure both SOA Domain Management Server and Tivoli Common Object Repository, click **Next** to continue that configuration. See "Configuring the Tivoli Common Object Repository."

6. If you are not configuring Tivoli Common Object Repository, exit the utility and rebuild and restart the Tivoli Enterprise Portal Server for the configuration to take effect. For the procedure, see "Rebuilding and restarting the Tivoli Enterprise Portal Server" on page 227. Reconfiguring Tivoli Enterprise Portal Server might take 5-10 minutes to complete. During this time the Manage Tivoli Enterprise Monitoring Services utility might appear to be inoperable.

For information about the additional steps required to verify the installation and to enable access to the ITCAM for SOA Navigator in the Tivoli Enterprise Portal, see Part 5, "Completing your installation," on page 495. Be sure to complete all of the installation and verification steps documented in this guide before using the product.

Configuring the Tivoli Common Object Repository: To configure SOA Domain Management Server, complete the following steps:

1. Start the `ConfigDMS` utility in graphical user interface mode, if it is not started. For more information, see "Running the `ConfigDMS` utility in Graphical User Interface mode" on page 200.
2. Specify whether to create the Tivoli Common Object Repository database locally, or whether to use an existing (local or remote) database that you have previously created.



Enter the following parameters for configuring the Tivoli Common Object Repository.

○ Create the Tivoli Common Object Repository database locally

● Use already existing database

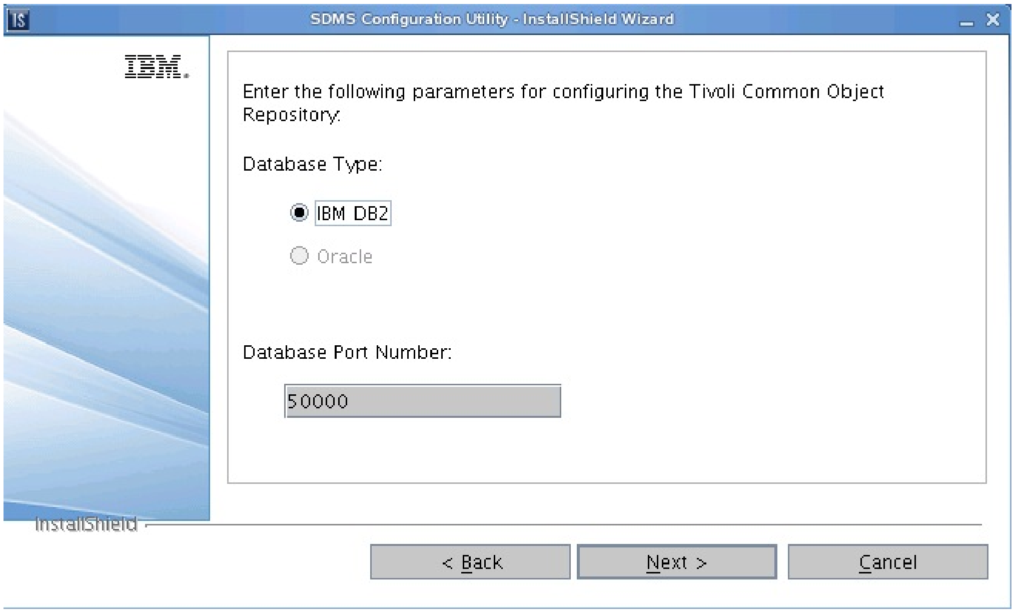
Database Hostname: localhost

Figure 48. Configuring the Tivoli Common Object Repository

If you prefer to use an existing local or remote database, select **Use an existing database** and enter the host name of the computer where the Tivoli Common Object Repository database is located. You can also specify *localhost* to use an existing local database.

Important: If you plan to use an Oracle database to support the Tivoli Common Object Repository, you must use an existing database that is either on the local portal server or is on a remote database server. You must also use an Oracle database for the SOA Domain Management Server.
If you are configuring a remote Tivoli Common Object Repository database that you previously created (for example, with the `make_db2_db.sh` script for a DB2 database), specify the fully qualified host name for the computer where the remote database server is located.

3. Select the database type.



SDMS Configuration Utility - InstallShield Wizard

Enter the following parameters for configuring the Tivoli Common Object Repository:

Database Type:

● IBM DB2

○ Oracle

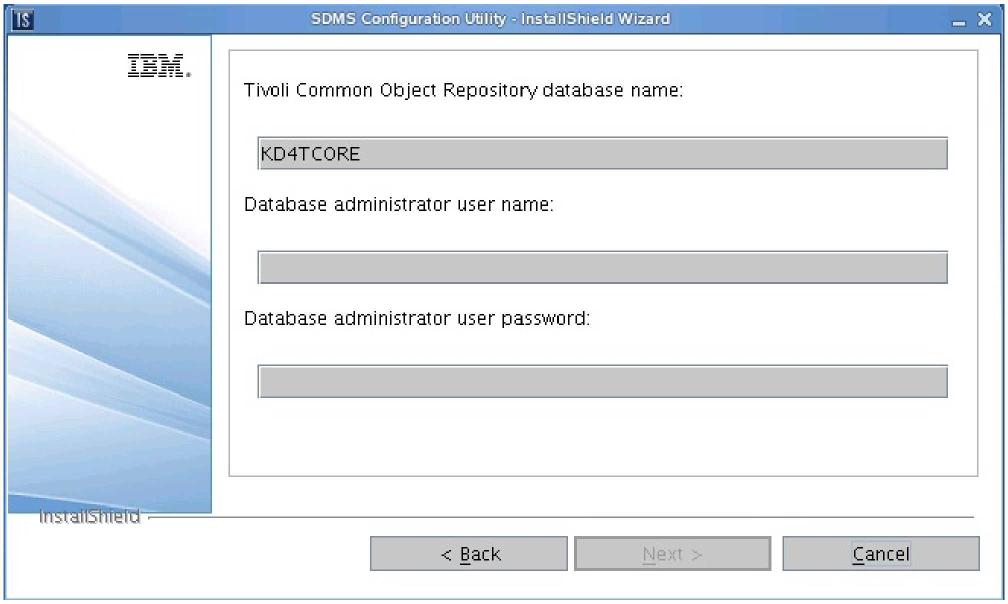
Database Port Number:

50000

Figure 49. Configuring the SOA Domain Management Server

If you are creating a database with the `ConfigDMS` utility, the option IBM DB2 is available for selection, and the option Oracle is unavailable. If you selected the option to use an existing database, both options are available for selection.

4. If you selected DB2 as the database type, complete the following steps:
   a. Enter the database port number. The default port number is `50000`.
   b. Enter the name of the Tivoli Common Object Repository database. The default name is `KD4TCORE` and has a limit of 8 characters.



Tivoli Common Object Repository database name:

KD4TCORE

Database administrator user name:

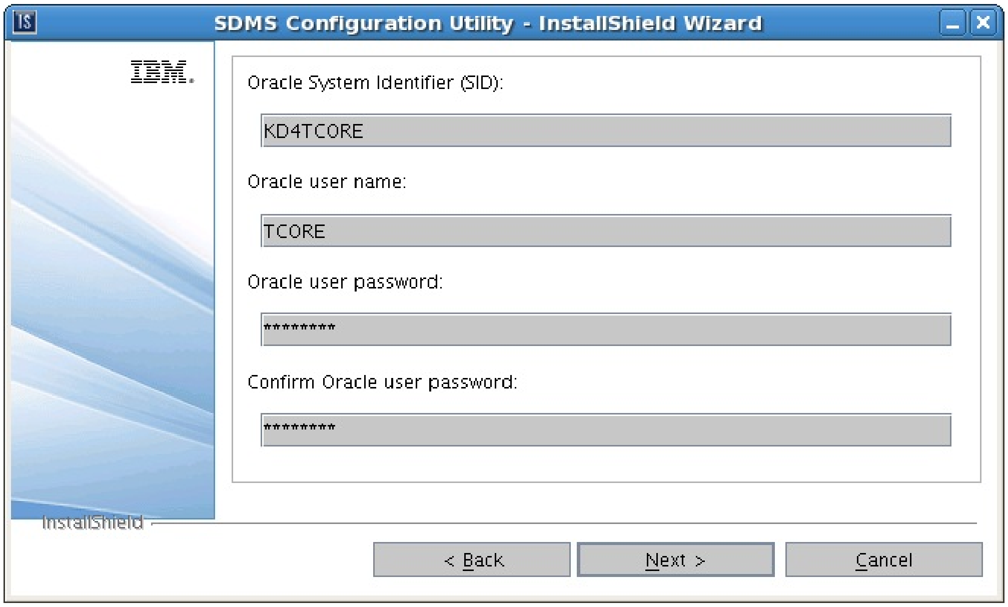
Database administrator user password:

Figure 50. Specifying the Tivoli Common Object Repository database name and database user

If you specified to create the Tivoli Common Object Repository database locally and this database name exists on the local system, it is dropped and re-created. If you want the configuration utility to create this database for you and you do not want to drop an existing database, specify a different name. Likewise, if you use the `ConfigDMS` utility to create a local database for the SOA Domain Management Server and a local database for the Tivoli Common Object Repository, you must specify different names for each database.

c. Enter the database administrative user name and password (for example, the default user name and password, *db2inst1*). This user name must exist, and the configuration utility validates the specified password before continuing. The password cannot contain the '$' symbol. For more information about the authorization required for this database user, see "Database and User Permissions" on page 178.

5. If you selected Oracle as the database type, complete the following steps:
   a. Enter the fully qualified host name of the Oracle database server.
   b. Enter the database port number. The default port number is *1521*.
   c. Enter Oracle system identifier. Set the Oracle system identifier to the system identifier specified when you ran the `make_ora_user.sh` script.



Oracle System Identifier (SID):

KD4TCORE

Oracle user name:

TCORE

Oracle user password:

****

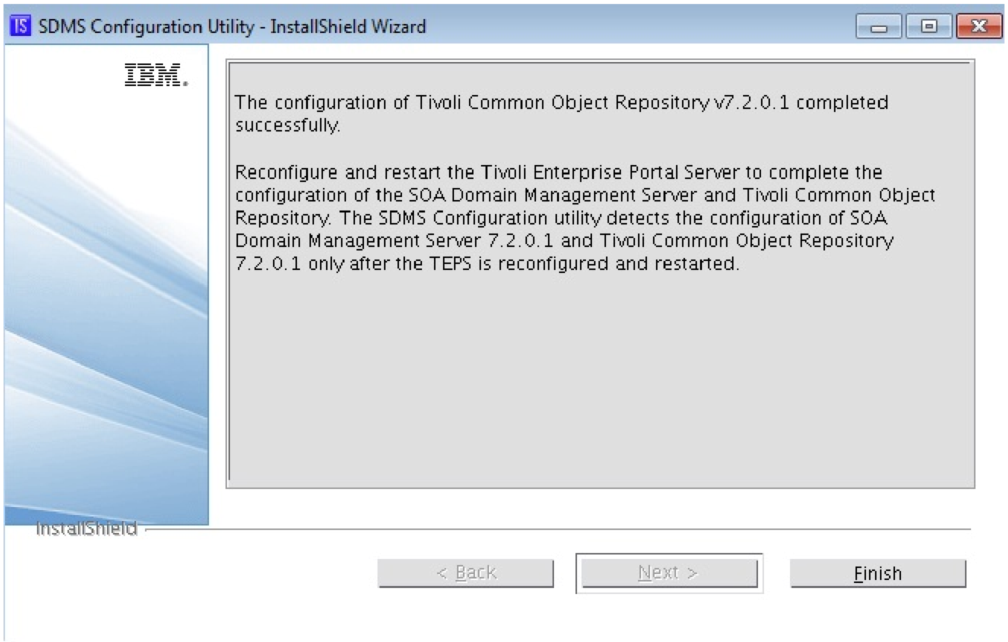
Confirm Oracle user password:

****

Figure 51. Specifying the Tivoli Common Object Repository Oracle System Identifier

   d. Enter the Oracle user name. Specify the Oracle user that was entered when you ran the `make_ora_user.sh` script.
   e. Enter the Oracle user password. Set the Oracle user password to the user password specified when you ran the `make_ora_user.sh` script. The password cannot contain the '$' symbol.
   f. The utility validates the specified user name and password.

6. The utility configures Tivoli Common Object Repository. If there are errors, you are notified and you can go back and correct any specified parameters, or you can exit the utility.
7. The utility informs you that the configuration is complete:


SDMS Configuration Utility - InstallShield Wizard

The configuration of Tivoli Common Object Repository v7.2.0.1 completed successfully.

Reconfigure and restart the Tivoli Enterprise Portal Server to complete the configuration of the SOA Domain Management Server and Tivoli Common Object Repository. The SDMS Configuration utility detects the configuration of SOA Domain Management Server 7.2.0.1 and Tivoli Common Object Repository 7.2.0.1 only after the TEPS is reconfigured and restarted.

Figure 52. Recommendation to rebuild and restart Tivoli Enterprise Portal Server

8. Click **Finish** to exit the utility.
9. Rebuild and restart Tivoli Enterprise Portal Server for the configuration to take effect. For the procedure, see “Rebuilding and restarting the Tivoli Enterprise Portal Server” on page 227. Reconfiguring Tivoli Enterprise Portal Server might take 5-10 minutes to complete. During this time the Manage Tivoli Enterprise Monitoring Services utility might appear to be inoperable.

For information about the additional steps required to verify the installation and to enable access to the ITCAM for SOA Navigator in the Tivoli Enterprise Portal, see Part 5, “Completing your installation,” on page 495. Be sure to complete all of the installation and verification steps documented in this guide before using the product.

Updating authentication using the ConfigDMS utility

You can update the SOA Domain Management Server authentication if the DB2 or Oracle password is changed in your database application.

Updating authentication for SOA Domain Management Server: To update the SOA Domain Management Server authentication for a DB2 or Oracle database, complete the following steps:

1. Stop the Tivoli Enterprise Portal Server.
2. Open a command prompt.
3. Run the `ConfigDMS` utility from the *`ITM_HOME`*/*`Platform`*`/cq/Products/KD4/bin` directory.

   For information about resolving directory path and platform variables, see “Resolving directory path variables” on page xvi.
4. Select **Update SOA Domain Management Server Authentication**.
5. Specify the new value in the field provided.

   The configuration utility verifies the new password by connecting to the database, and you are notified of any errors. You can return to the previous configuration utility page and correct your input before trying again. The password cannot contain the ’$’ symbol.

6. Exit the utility.
7. Start the Tivoli Enterprise Portal Server.

   You do not have to rebuild the Tivoli Enterprise Portal Server configuration after updating the authentication, but you do have to restart the Tivoli Enterprise Portal Server for the authentication update to take effect.

Updating authentication for Tivoli Common Object Repository: You can update the Tivoli Common Object Repository authentication if the DB2 or Oracle password is changed in your database application.

To update the Tivoli Common Object Repository authentication for a DB2 database, complete the following steps:

1. Stop the Tivoli Enterprise Portal Server.
2. Open a command prompt.
3. Run the `ConfigDMS` utility from the *`ITM_HOME`*/*`Platform`*`/cq/Products/KD4/bin` directory.

   For information about resolving directory path and platform variables, see “Resolving directory path variables” on page xvi.
4. Select **Update Tivoli Common Object Repository Authentication**.
5. Specify the new value in the field provided.

   The configuration utility verifies the new password by connecting to the database, and you are notified of any errors. You can return to the previous configuration utility page to correct your input before trying again.
6. Exit the utility.
7. Start the Tivoli Enterprise Portal Server.

   You do not have to rebuild the Tivoli Enterprise Portal Server configuration after updating the authentication, but you do must restart the Tivoli Enterprise Portal Server for the authentication update to take effect.

Running the `ConfigDMS` utility in console mode

Running the `ConfigDMS` utility with the `–console` option starts the `ConfigDMS` utility in the command line.

You are prompted to select a language, and then a welcome response is displayed in the command line processor window, and you are prompted to continue by typing a numerical response:

- Type `1` to continue.
- Type `3` to cancel the wizard.
- Type `5` to display the response message and your choices again.

Throughout the use of the wizard in console mode, you must respond by typing one of several valid responses. The wizard presents the same basic selection options as described in “Running the `ConfigDMS` utility in Graphical User Interface mode” on page 200.

Rebuild and restart the Tivoli Enterprise Portal Server

After exiting the utility, if you only updated authentication, you must restart Tivoli Enterprise Portal Server for the update to take effect. If you configured or upgraded support for SOA Domain Management Server or Tivoli Common Object

Repository, you must rebuild and restart the Tivoli Enterprise Portal Server configuration for the configuration to take effect. For the procedure, see "Rebuilding and restarting the Tivoli Enterprise Portal Server" on page 227.

Running the ConfigDMS utility in silent mode

Running the ConfigDMS utility with the**–silent [*dir_path/*]*silent_file*** option starts the ConfigDMS utility in silent mode, using properties defined in the *silent_file* properties file.

Restriction: You cannot use the –silent mode and –console mode together.

When you run the ConfigDMS utility in silent mode, the configuration parameters are read from a simple text properties file, *silent_file*, that you create in advance. A typical properties file might look similar to the following example:

```
# Sample silent configuration file - silent file to deploy SDMS and TCORE
# File version - make sure that you are using proper version of silent file.
version=7.20.01.00

config_sdms=yes
config_tcore=no
update_sdms_auth=no
update_tcore_auth=no
update_sdms=no
update_tcore=no
upgrade=no

# SDMS section
# Supported values on Linux and AIX are "db2" and "oracle"
# For an existing, remote database you may also set "mssql2005" for
MS SQL 2005 or 2008
sdms_db_type=db2
# Use default port - uncomment the property to set to a different value
#sdms_db_port=

# Sample JDBC path when SDMS is configured to use DB2
sdms_jdbc_path=/home/db2inst1/sqllib/java/db2jcc.jar;/home/db2inst1/sqllib
/java/db2jcc_license_cu.jar

# Sample JDBC path when SDMS is configured to use an existing,
remote MS SQL 2005 or 2008
# sdms_jdbc_path=/tmp/Microsoft_SQL_Server_2005_JDBC_Driver/
sqljdbc_1.2/enu/sqljdbc.jar

# Sample JDBC path when SDMS is configured to use ORACLE. The location of the
Oracle 10g Release 2 JDBC driver must be specified.
# sdms_jdbc_path=/oracle-jdbc-driver/ojdbc6.jar

# Supported values are:
# 'yes' if SDMS database need to be created locally. 'yes' is not supported when
sdms_db_type is set to "oracle"
# 'no'  if SDMS is configured to use existing database
sdms_db_create_locally=yes

# When the database type is Oracle, this property specifies the
Oracle System Identifier (SID)
sdms_db_name=KD4SDMS

# When the database type is Oracle, this property is ignored and SDMS is
used as the Oracle database user name.
sdms_db_user=sdms
sdms_db_password=secret1

# Uncomment this property when SDMS is configured to use existing database
# on host different then 'localhost'
# sdms_db_host=localhost

# Uncomment this property when SDMS is configured to MS SQL 2005 or 2008 and
# instance other than default should be used. Instance name should be in
form hostname\instance_name
# sdms_mssql_instance=hostname\\sample_instance

# TCORE section
# Supported values on AIX and Linux are "db2" and "oracle"
# IMPORTANT:  When "oracle" is specified , the sdms_db_type property
must also be set to "oracle".
tcore_db_type=db2

# Supported values are:
# 'yes' if TCORE database need to be created locally. 'yes' is not
supported when tcore_db_type is set to "oracle"
# 'no'  if TCORE is configured to use existing database
tcore_db_create_locally=yes

# Uncomment this property when TCORE is configured to use existing database
# on host different then 'localhost'
# tcore_db_host=localhost

# Use default port - uncomment the property to set to a different value
#tcore_db_port=
tcore_db_name=KD4TCORE
tcore_db_user=tcore
tcore_db_password=secret1
```

Remember: Make sure that you use the version of the file from ITCAM for SOA version 7.2 Fix Pack 1.

When you create a silent response properties file, keep in mind these considerations:

- A line in the file that starts with the # character is treated as a comment, and is not processed. If the # character is used elsewhere in the line, it is not considered to be the start of a comment. This means that you can use the # character in passwords or for other uses. The password cannot contain the '$' symbol.
- The properties file is coded with the ISO 8859-1 character set.
- The properties file can include only one *version* property. For ITCAM for SOA version 7.2 Fix Pack 1, the only valid value of this property is the predefined value *07.20.01.00*.
- Each property is described on a separate line, in the following format: *Property* = *value*.

  Property
  This is the name of property. The list of valid properties that you can configure is shown in Table 28 on page 221.

  Value This is the value of the property. Default values for some properties are already provided. You can erase default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can simply comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case-sensitive.
- Sample properties files (sample_silent_unix.cfg and sample_silent_win.cfg) are packaged with the SOA Domain Management Server Configuration utility.

Depending on your operating system, these files are available in one of these directories, where *ITM_Home* is the location where IBM Tivoli Monitoring is installed (For information about resolving directory path and platform variables, see "Resolving directory path variables" on page xvi.)

***ITM_Home*/*platform*/cq/Products/KD4/latest/bin**

Table 28. Available properties for running the SOA Domain Management Server Configuration utility in silent mode

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
version	Yes				Version number of the properties file, and must be set to the value of *7.20.01.00*.
config_sdms	No	*yes* or *no*			Specifies whether to configure SOA Domain Management Server. If this property is not specified, the default value of *No* is assumed.
config_tcore	No	*yes* or *no*			Specifies whether to configure the Tivoli Common Object Repository. If this property is not specified, the default value of *No* is assumed.
update_sdms	No	*yes* or *no*			Specifies whether to update the configuration of SOA Domain Management Server to the latest version when a fix pack or interim fix is installed. If this property is not specified, the default value of *No* is assumed.
update_tcore	No	*yes* or *no*			Specifies whether to update the configuration of Tivoli Common Object Repository to the latest version when a fix pack or interim fix is installed. If this property is not specified, the default value of *No* is assumed.
update_sdms_auth	No	*yes* or *no*			Specifies whether to update the authentication for SOA Domain Management Server by changing the database password. If this property is not specified, the default value of *No* is assumed
update_tcore_auth	No	*yes* or *no*			Specifies whether to update the authentication for Tivoli Common Object Repository by changing the database password. If this property is not specified, the default value of *No* is assumed

Table 28. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
upgrade	No	*yes* or *no*	X	X	Specifies whether to upgrade or update a previous configuration of SOA Domain Management Server and Tivoli Common Object Repository to version 7.2 or version 7.2 Fix Pack 1, depending on already configured components. If this property is not specified, the default value of *No* is assumed.
sdms_db_type	No	*db2* , *mssql2005* or *oracle*			Specifies the type of database server that is used for the SOA Domain Management Server database. If this property is not specified, the value is obtained from the Tivoli Enterprise Portal Server configuration.
sdms_jdbc_path	Yes when the *config_sdms* property has the value of *Yes*				Specifies the fully qualified directory paths where the JDBC driver class files for the SOA Domain Management Server database that are being created are located. To include more than one directory path and JAR file, separate them in the list with a semicolon. For the list of JDBC driver class files required for DB2,Microsoft SQL Server, or Oracle, see "Configuring the SOA Domain Management Server" on page 208. **Important:** When configuring or upgrading an Oracle database (Oracle 10g Release 2, Oracle 11g Release 1, or Oracle 11g Release 2), the `ojdbc6.jar` must be used as the JDBC driver. See technote.
sdms_db_create_locally	Yes	*yes* or *no*			Specifies whether the configuration utility must create the SOA Domain Management Server database locally (*yes*) or use an existing (local or remote) SOA Domain Management Server database (*no*). The value must be set to *no* if the database type is Oracle.

Table 28. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
sdms_db_name	No				For DB2 database, specifies the name of the SOA Domain Management Server database that is being created. For DB2, the name can be a maximum of 8 characters. If this property is not specified, the default value of *KD4SDMS* is assumed. **Remember:** If this database exists, it is dropped and re-created. If you do not want to drop an existing database, specify a different name. For Oracle, this parameter is set to the Object System Identifier (SID) that was specified when you ran the `Kd4InitOracleDb` script.
sdms_db_user	Yes when the *config_sdms* property has the value of *Yes*				Specifies the DB2 administrative database user name that is authorized to access the SOA Domain Management Server database. For more information about authorization required for this user, see "Database and User Permissions" on page 178. For Oracle, this property is ignored as *SDMS* is always used as the Oracle user name.
sdms_db_password	Yes, in these cases: • the *config_sdms* property has the value of *Yes* • the *update_sdms_auth* property has the value of *Yes*				Specifies the database password associated with the user name specified in the *sdms_db_user* property.

Table 28. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
sdms_db_host	Yes, if your SOA Domain Management Server database is on a computer other than where Tivoli Enterprise Portal Server is installed.	Fully qualified host name or *localhost*			Specifies the host name for the database server computer where the SOA Domain Management Server database is located. If your database is on a computer other than where Tivoli Enterprise Portal Server is installed, specify the fully qualified remote hostname. If this property is not specified, the default value of *localhost* is used.
tcore_db_type	Yes	*db2* or *oracle*			Specifies the type of database server that is used for the Tivoli Common Object Repository database. When *oracle* is specified, the property `sdms_db_type` must also be set to *oracle*.
tcore_db_create_locally	Yes	*yes* or *no*			For DB2, this property specifies whether the configuration utility creates the Tivoli Common Object Repository database locally (*yes*) or uses an existing (local or remote) Tivoli Common Object Repository database (*no*). The value must be set to *no* if the database type is Oracle.
tcore_db_host	Yes, if your Tivoli Common Object Repository database is on a computer other than where Tivoli Enterprise Portal Server is installed.	Fully qualified host name or *localhost*			Specifies the host name for the database server computer where the Tivoli Common Object Repository database is located. If your database is on a computer other than where Tivoli Enterprise Portal Server is installed, specify the fully qualified remote hostname. If this property is not specified, the default value of *localhost* is used.
tcore_db_port	No				This property specifies the port number for the Tivoli Common Object Repository database. If this property is not specified, the default value of *50000* for a DB2 database or *1521* for an Oracle database is assumed.

Table 28. Available properties for running the SOA Domain Management Server Configuration utility in silent mode (continued)

Property	Required (Yes/No)	Possible values	Upgrade of SDMS only	Upgrade of SDMS and TCORE	Comment
tcore_db_name	No				Specifies the name of the Tivoli Common Object Repository database. For DB2, if this property is not specified, the default value of *KD4TCORE* is assumed. The name can be a maximum of 8 characters. **Remember:** If you specified to create the database locally and this database exists, it is dropped and re-created. If you do not want to drop an existing database, specify a different name. For Oracle, specify the Oracle System Identifier that was specified when you ran the `make_ora_user` script.
tcore_db_user	Yes, if *config_tcore* has the value of *Yes*				Specifies the administrative database user name that is authorized to create and access the Tivoli Common Object Repository database. For more information about the authorization required for this user, see "Database and User Permissions" on page 178.
tcore_db_password	Yes, if *config_tcore* or *update_tcore_ auth* has the value of *Yes*				This property specifies the database password associated with the user name specified in the *tcore_db_user* property.

Combining silent operations

When you are installing or upgrading to ITCAM for SOA version 7.2, if you create a silent response file to contain more than one operation (for example, configure Tivoli Common Object Repository and update SOA Domain Management Server), the operations are always completed in the following sequence:

1. Upgrade from version 7.1.1 to 7.2.
2. Configure SOA Domain Management Server
3. Configure Tivoli Common Object Repository
4. Update SOA Domain Management Server authentication credentials
5. Update Tivoli Common Object Repository authentication credentials

When you are updating to ITCAM for SOA version 7.2 Fix Pack 1, if you create a silent response file to contain more than one operation, the operations are always performed in the following sequence:

1. Upgrade from version 7.2 to 7.2 Fix Pack 1.
2. Configure SOA Domain Management Server
3. Configure Tivoli Common Object Repository
4. Update SOA Domain Management Server authentication credentials
5. Update Tivoli Common Object Repository authentication credentials

Some operations are mutually exclusive, and cannot be defined in the same silent response file. These operations can be completed with the same silent response file:

- config_sdms and config_tcore
- update_sdms and config_tcore
- update_sdms and update_tcore
- update_sdms_auth and update_tcore_auth

Silent mode errors and messages

The `ConfigDMS` utility validates the operations and their values in the silent response file and displays a message when required values are missing or when a property is assigned a value that is not valid.

The `ConfigDMS` utility displays messages that describe the operations that are being performed by the utility and results of those operations (success or failure). When an error occurs, the error code and the error message are displayed describing the cause of the failure, if possible.

If the silent response file contains several operations that can be performed from the same file, the first error that occurs stops the `ConfigDMS` utility. For example, if you are configuring both SOA Domain Management Server and Tivoli Common Object Repository and an error occurs during the configuration of SOA Domain Management Server, the SOA Domain Management Server Configuration utility does not start the configuration of Tivoli Common Object Repository.

After the configuration or upgrade of SOA Domain Management Server or Tivoli Common Object Repository completes, you must rebuild and restart the Tivoli Enterprise Portal Server. This reconfiguration can take some time to complete. Be sure to wait for completion before attempting to run the `ConfigDMS` utility again. If you are updating authentication credentials only, you need to restart Tivoli Enterprise Portal Server only.

Increasing the report request limit on the portal server

The report request limit that is specified in the portal server environment file defines the normal limit of pending report requests to the portal server from a single client. This parameter is set to 50 by default. In an IBM Business Process Manager server environment, in particular, if many application servers are monitored on a single application server host, this limit might be exceeded. If you plan to configure data collection for multiple application servers, increase the report request limit to 100.

1. Navigate to the *ITM_Home*/config/cq.ini file.
2. Add or set the property KFW_REPORT_REQUEST_LIMIT to 100. For example:
   ```
   KFW_REPORT_REQUEST_LIMIT=100
   ```
3. Save the changes to the cq.ini file.
4. Restart the portal server.

Rebuilding and restarting the Tivoli Enterprise Portal Server

After the `ConfigDMS` utility completes the tasks of upgrading, configuring, or updating SOA Domain Management Server or Tivoli Common Object Repository, rebuild the Tivoli Enterprise Portal Server configuration.

Important: If you are only *updating the authentication credentials*, you do not have to rebuild the portal server configuration, but you do must restart the portal server for the changes to take effect.

To rebuild the portal server configuration, complete these steps:

1. Change to the `*ITM_Home*/bin` directory.
2. Enter the following command to open the Manage Tivoli Enterprise Monitoring Services utility: `./itmcmd manage`
3. Verify that the Tivoli Enterprise Portal Server is started.
4. Right-click **Tivoli Enterprise Portal Server**.
5. In the menu, click **Rebuild Configuration**.

For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.

Remember: The first time that you configure SOA Domain Management Server and Tivoli Common Object Repository, rebuilding the portal server takes at least 5 - 15 minutes to complete, and during this time the Manage Tivoli Enterprise Monitoring Services console might appear to be inoperable.

Chapter 6. Installing the ITCAM for SOA SDMS agent

The ITCAM for SOA SDMS agent is provided as part of an ITCAM for SOA 7.2 Fix Pack 1 or later installation.

Important: The ITCAM for SOA SDMS agent is only required if you want to view Business Process Management monitoring data in IBM SmartCloud™ Application Performance Management UI version 7.6 or later.

For more information about IBM SmartCloud™ Application Performance Management UI, see the *IBM SmartCloud Application Performance Management User Interface User's Guide*.

The agent provides minimal user-visible content in the Tivoli Enterprise Portal. No agent-specific workspaces, situations, or take action commands are provided. The attribute groups are designed to provide a data interface to the Application Performance Management UI rather than for use in the Tivoli Enterprise Portal.

For more information about the ITCAM for SOA SDMS agent attribute groups, see the "ITCAM for SOA SDMS Agent attribute groups" appendix in the *IBM Tivoli Composite Application Manager for SOA User's Guide*.

Before you install the ITCAM for SOA SDMS agent version 7.2 Fix Pack 1, review the software requirements for the agent in "Required software" on page 15.

Important: Installing the ITCAM for SOA SDMS agent upgrades Tivoli Monitoring to version 6.2.3 fix pack 1.

The agent can remotely query SOA Domain Management Server data, so you can install the agent on a separate system from the Tivoli Enterprise Portal Server.

Installing and configuring the ITCAM for SOA SDMS agent on Windows systems

If a previous version of the ITCAM for SOA SDMS agent is installed, you must uninstall this version and reinstall ITCAM for SOA SDMS agent version 7.2 Fix Pack 1. To uninstall the ITCAM for SOA SDMS agent, complete the procedure that is documented in "Uninstalling the monitoring agent on Windows systems" on page 237.

Permissions for installing the ITCAM for SOA SDMS monitoring agent

To install the ITCAM for SOA SDMS monitoring agent, you must have the following permissions:

- You must have administrator privileges on the computer system where the monitoring agent is being installed.
- You must run the monitoring agent as a user with administrator privileges.
- All IBM Tivoli Monitoring components, including the monitoring agent, must be installed and run as the same user. For more information about permissions, see the User Authority section of the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Enabling application support on the monitoring server, portal server, and portal client

To ensure the ITCAM for SOA SDMS agent works within your Tivoli Monitoring infrastructure, application support files must be distributed to the Tivoli Monitoring components.

Application support files are automatically installed and enabled on the monitoring servers and the portal server, if the agent and the monitoring servers are enabled for self-description. ITCAM for SOA SDMS agent is enabled by default for self-description. For more information, see "Enabling application support through self-description."

If the agent and the Tivoli Monitoring components are not enabled for self-description, you must manually install application support files on the Tivoli Monitoring components. For more information, see "Installing and enabling application support manually before installing the agent" on page 37.

Enabling application support through self-description

When the ITCAM for SOA SDMS agent is installed and the monitoring servers and portal server are enabled for self-description, application support files are automatically installed on the monitoring servers and the portal server without the need to recycle the portal server and the monitoring server. Application support files must be installed manually on the portal client.

To verify that the application support files are installed, open a command prompt and issue the `Kincinfo -t` command. The output lists the application support files that are installed. For example:

```
PC  PRODUCT DESC                                  PLAT
VER         BUILD        INSTALL DATE
S4  Monitoring Agent for ITCAM for SOA SDMS       WICNS
07.20.01.00  201303251100  20130326 1036
S4  Monitoring Agent for ITCAM for SOA SDMS       WIXEB
07.20.01.00  201303251100  20130326 1036
S4 Monitoring Agent for ITCAM for SOA SDMS        WIXEW
07.20.01.00  201303251100  20130326 1036
```

The self-describing agent feature is disabled by default on the hub monitoring server. The procedure for enabling self-description on the hub monitoring server is documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing and enabling application support manually before you install the agent

The following procedures refer to adding application support when the Tivoli Monitoring components are installed on a separate computer system to the monitoring agent. If the ITCAM for SOA SDMS agent and the Tivoli Monitoring components are on the same computer system, you install application support files when you install the agent.

When all of the Tivoli Monitoring components are on the same computer system, support files for each of the monitoring components must be installed at the same time.

When you manually install application support on your Tivoli Enterprise Monitoring Server, you must be logged in as the user who installed the Tivoli Enterprise Monitoring Server.

The Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal must be stopped before you install the application support files. To stop Tivoli Monitoring components, complete the following steps:

1. Launch Manage Tivoli Enterprise Monitoring Services.
2. Right-click the component that you want to stop.
3. Click **Stop** from the menu.

Complete the following steps to manually install application support for the ITCAM for SOA SDMS agent on a single computer:

1. When you load the ITCAM for SOA installation media, navigate to the `KS4` directory and extract the archive file for the ITCAM for SOA SDMS agent.
2. Navigate to the `*KS4_extract_folder*\KS4\WINDOWS` directory and double-click the `setup.exe` file.
3. On the Welcome page, click **Next**.
4. The Software License Agreement page is displayed. Accept the license agreement and click **Next**.
5. From the Select Features page, select **Tivoli Enterprise Monitoring Server - TEMS**, **Tivoli Enterprise Portal Server - TEPS**, and **TEP Desktop client -TEPD** and click **Next**.
6. The Agent Deployment page provides an option to install the Tivoli Enterprise Monitoring Agent remotely. Click **Next** without selecting the **Monitoring Agent for ITCAM for SOA SDMS** check box.
   For more information about remote deployment of the monitoring agent, see "Configuring for remote deployment of the monitoring agent" on page 63.
7. Review the installation summary details and click **Next** to start the installation.
   The application support packages for the monitoring server, portal server, and portal desktop client are installed.
8. On the Setup Type window, complete the following steps:
   a. Select the **Install application support for a local/remote Tivoli Enterprise Monitoring Server** check box.
   b. (Optional) Select the check box for launching the Manage Tivoli Enterprise Monitoring Servers window. (If selected, this window is displayed when the installation procedure is finished.)
   c. (Optional) Select the check box for configuring the default connection from the monitoring agent to the Tivoli Enterprise Monitoring Server.

   The option for configuring the Tivoli Enterprise Portal is mandatory (preceded by an asterisk [*]) and cannot be cleared.
   Click **Next**.
9. The TEPS Hostname window is displayed. The host name for the local computer is displayed. Accept the default value and click **Next**.
10. To activate application support on the monitoring server, specify the location of the monitoring server. In the **Add application support to the TEMS** window, select **On this computer** and click **OK**.
11. Select the application support component that you want to add to the monitoring server and click **OK**.
    By default, the application support for **Monitoring Agent for ITCAM for SOA SDMS** is already selected.
12. Click **Next** on the message that provides the results of the process of adding application support.

13. The InstallShield Wizard Complete page is displayed indicating that the installation was successful, and providing an option to view the readme file for the product. Click **Finish**.
14. If you selected the **Launch Manage Tivoli Monitoring Services** check box in 8 on page 231, the Manage Tivoli Enterprise Monitoring Services utility opens.
15. Restart Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal. Complete these steps:
    a. Launch Manage Tivoli Enterprise Monitoring Services.
    b. Right-click the component that you want to start.
    c. Click **Start** from the menu.

Installing and Configuring the ITCAM for SOA SDMS agent on Windows

Complete the following procedure to install and configure the ITCAM for SOA SDMS agent on Windows.

Before you begin

This installation of the ITCAM for SOA SDMS agent is based on the following assumptions:

- You installed or upgraded your Tivoli Monitoring environment to one of the minimum supported levels (see "Software and hardware prerequisites" on page 15).
- You already installed ITCAM for SOA SDMS application support for the Tivoli Monitoring components. For more information about installing application support, see "Enabling application support on the monitoring server, portal server, and portal client" on page 230. If your IBM Tivoli Monitoring components are installed on the same computer systems as your application server runtime environment, application support can be installed during the installation of the monitoring agent.

The appropriate level of the Tivoli Enterprise Management Agent Framework is installed when the monitoring agent is installed.

About this task

The ITCAM for SOA SDMS agent can remotely query SOA Domain Management Server data, so you can install the agent on a separate system from the Tivoli Enterprise Portal Server.

Procedure

1. When you load the ITCAM for SOA installation media, navigate to the `KS4` directory and extract the archive file for the ITCAM for SOA SDMS agent.
2. Navigate to the `*KS4_extract_folder*\KS4\WINDOWS` directory and double-click the `setup.exe` file.
3. Click **Next**. The ITCAM for SOA SDMS agent prerequisites are displayed.
4. Click **Next**. The Software License Agreement is displayed.
5. Read the license agreement and click **Accept**. The **Choose destination location** window opens.
6. Choose the directory where you want to install the ITCAM for SOA SDMS agent. If you installed IBM Tivoli Monitoring components on the same server, the destination directory is determined automatically and this step is skipped.

To use a location other than the default (C:\IBM\ITM), click **Browse** and select the folder that you want to use. Click **Next**. If IBM Tivoli Monitoring components are not already installed, the **User Data Encryption Key** page opens.

7. The 32-character encryption key is used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment: A default value, IBMTivoliMonitoringEncryptionKey, is displayed. Either accept the default value or enter your own 32-character encryption key. This key must be the same as the key that was used during the installation of the monitoring server to which this monitoring agent connects. Click **Next**. Click **OK** to confirm the encryption key. The **Select Features** window is displayed.
8. Expand Tivoli Enterprise Monitoring Agents, and select **ITCAM for SOA SDMS agent**. If you are installing the ITCAM for SOA SDMS agent on a Windows 64-bit system, two additional features are available for selection:
   - 32/64 Bit Agent Compatibility Package (x86-64 only)
   - Tivoli Enterprise Monitoring Agent Framework (x86-64 only)

   The Agent Compatibility Package provides support for installing 32-bit agents on a system where 64-bit agents are installed. The 32/64 Bit Agent Compatibility Package (x86-64 only) and Tivoli Enterprise Monitoring Agent Framework (x86-64 only) options are automatically selected if the following conditions are met:
   - You are installing on a 64-bit system.
   - Another 64-bit agent is installed on the system.
   - The 32/64 Bit Agent Compatibility Package is not already installed.

   Click **Next**.
9. If no IBM Tivoli Monitoring component was previously installed on this computer, a window is displayed for you to select an IBM Tivoli Monitoring program folder for the Windows Start menu. The default program folder name is IBM Tivoli Monitoring. Select a program folder and click **Next**.
10. If you are installing the ITCAM for SOA SDMS agent on a computer that already has a monitoring server installed, the **Agent Deployment** window is displayed. It lists the agents on the installation image that you can add to the agent depot. The agent depot contains agents that you can deploy to remote computers. Select the agent that you want to add to the agent depot. By default, the agent depot is in the itm_installdir\CMS\depot directory. If you want to use a different directory, specify the directory using the DEPOTHOME key in the KBBENV file. For information about how to deploy agents in the agent depot to remote computers, see the *IBM Tivoli Installation guide*. Click **Next**.
11. Review the installation summary details. Click **Next** to start the installation. After the installation is complete, the Setup Type window is displayed.
12. Choose whether to start the Manage Tivoli Enterprise Monitoring Servers window and the Tivoli Enterprise Monitoring Server Configuration window. Click **Next**
13. If you selected the option to configuration the default connection to the monitoring server, the Tivoli Enterprise Monitoring Server Configuration window is displayed.
14. In the configuration window, define the communications between the monitoring agents and the monitoring server:
    a. If the agents must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.

b. Identify the type of protocol that the agents use to communicate with the monitoring server. There are four choices available: IP.UDP, IP.PIPE, IP.SPIPE, or SNA. You can specify up to three methods for communication. If the method you specify as protocol 1 fails, protocol 2 is used. If protocol 2 fails, protocol 3 is used.

   Note: Do not select **Optional Secondary TEMS Connection**. You can set up the failover support for agents after installation, this set up is described in the *IBM Tivoli Monitoring: High-Availability Guide for Distributed Systems*.

c. Complete the fields for the protocol/s that you specified.

Table 29. IP.UDP, IP.PIPE, IP.SPIPE, and SNA field descriptions

Field	Description
IP.UDP Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port # or Port Pools	The listening port for the hub monitoring server. The default number is 1918.
IP.PIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port Number	The listening port for the monitoring server. The default number is 1918.
IP.SPIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port number	The listening port for the hub monitoring server. The default value is 3660.
SNA Settings	
Network Name	The SNA network identifier for your location.
LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
LU 6.2 LOGMODE	The name of the LU6.2 LOGMODE. The default value is `CANCTDCS`.
TP Name	The transaction program name for the monitoring server.
Local LU Alias	Local LU Alias

d. Click **OK**. For additional information about these parameters, click **Help**.

15. A configuration window opens. Enter configuration details for the ITCAM for SOA SDMS agent as described in the following table:

Table 30. Configuration parameters for ITCAM for SOA SDMS agent

Field	Description
`TEPS (SDMS) Server Host Name`	The host name of the Tivoli Enterprise Portal Server in which the SOA Domain Management Server is installed. The default value is `localhost`.
`User ID (e.g. sysadmin)`	User ID that is used to connect to SOA Domain Management Server, for example, `sysadmin`.

Table 30. Configuration parameters for ITCAM for SOA SDMS agent (continued)

Field	Description
`Password`	Password for the user ID that is being used to connect to SOA Domain Management Server.
`Background Collection Interval (in seconds)`	Background collection interval in seconds for data from SOA Domain Management Server. If you enter a value equal to or less than 0, the agent reverts to the default collection interval of 300 seconds.
`Java_home`	The path to where an IBM Java Runtime Environment (JRE) is installed. By default, the `Java_home` parameter is not set. If you encounter problems with the default JRE that is used by the agent, you can specify a value for `Java_home`. If you set a value for `Java_home`, you must specify the location of an IBM JRE, Java version 6 or later. The ITCAM for SOA SDMS agent looks for the Java executable in the directory *`JAVA_HOME`*`/bin`.

Click **OK**.

16. Click **Finish** to complete the installation.

What to do next

To configure the ITCAM for SOA SDMS monitoring agent, see "Configuring the monitoring agent" on page 58.

Silent installation on Windows systems

In addition to installing the ITCAM for SOA SDMS agent interactively, the installer supports a silent mode. In this mode, no user interaction is required for an installation or uninstallation. Instead, the parameters are taken from a *response* file. You can install and uninstall the ITCAM for SOA SDMS agent and install application support files in silent mode.

Important: You must stop any application servers that are configured by the ITCAM Data Collector for WebSphere before you perform a silent installation of the ITCAM for SOA SDMS agent.

Response files have a text format. You can create a response file based on one of the samples that are provided on the installation DVD or image.

You can also create a response file during installation, modify it if necessary, and then use it for a silent installation. In this way, you can reproduce similar configuration many times, for example, on different hosts.

Preparing response files on Windows systems

You can use the installer to install or uninstall the ITCAM for SOA SDMS agent in silent mode. Modify the sample response files that are on the installation DVD or image, and then run the installer from the command line.

To perform a silent installation or uninstallation of the ITCAM for SOA monitoring agent, you must first prepare the response file. Then, run the installer, supplying the name of the response file.

Preparing the response file for ITCAM for SOA SDMS agent installation

To prepare a response file for installing the ITCAM for SOA SDMS agent, complete the following procedure:

1. On the product installation DVD or image, in the `KS4_extract_folder\WINDOWS` directory, locate the `silent.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify and uncomment any of the following properties, if necessary:

Table 31. ITCAM for SOA installation response file properties

Parameter	Definition
License Agreement	Required. You must agree to the license agreement to proceed with the installation.
Install Directory	Required. Assign the full path name of the directory for the monitoring agent if it is different from the default. The default is `C:\IBM\ITM`. If you are installing on a computer where the monitoring agent is already installed, the current directory is used regardless of what you specify here.
Install Folder	Assign the name of the folder that is displayed in the Windows **Start** > **Programs** menu. Use this option if you want to use a folder name different from the default.
EncryptionKey	Required. The data encryption key that is used to encrypt the data that is sent between systems. This key must be the same for all components in your Tivoli Monitoring environment.
KS4WICMA	Required. Uncomment this property to install the ITCAM for SOA SDMS agent.

4. Save the edited copy in a work directory, for example, as `C:\TEMP\silent_install.txt`.

Preparing a response file for application support files installation

To prepare a response file for installing the support files on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal client, complete the following procedure:

1. On the product installation DVD or image, in the `KS4_extract_folder\WINDOWS` directory, locate the `silent.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Find the following lines, and uncomment the lines that apply to the host that you are installing on:

```
KS4WICMS=ITCAM for SOA SDMS Support ( TEMS )
KS4WIXEW=ITCAM for SOA SDMS Support ( TEP Workstation )
KS4WICNS=ITCAM for SOA SDMS Support ( TEP Server )
```

4. Save the edited copy in a work directory, for example, as `C:\TEMP\silent_install.txt`.

Preparing the response file for ITCAM for SOA SDMS agent uninstallation

To prepare a response file for uninstallation of the ITCAM for SOA SDMS agent, complete the following steps:

1. On the product installation DVD or image, in the *KS4_extract_folder*\WINDOWS directory, locate the `silent` file.
2. Make a copy of this file, and open it in a text editor.
3. Uncomment the following properties, if necessary:

Table 32. ITCAM for SOA installation response file properties

Parameter	Definition
UNINSTALLSELECTED=YES	Uncomment this property to uninstall components that are not Tivoli Monitoring specific.
KS4WICMS	Uncomment this property to uninstall the ITCAM for SOA SDMS agent application support files for the monitoring server.
KS4WIXEW	Uncomment this property to uninstall the ITCAM for SOA SDMS agent application support files for the portal client.
KS4WICNS	Uncomment this property to uninstall the ITCAM for SOA SDMS agent application support files for the portal server.
KS4WICNS	Uncomment this property to uninstall the ITCAM for SOA SDMS agent.

4. Save the edited copy in a work directory, for example, as `C:\TEMP\silent_install.txt`.

Running the silent installation or uninstallation

For the procedure for running the silent installation or uninstallation from a command prompt, see "Running the silent installation from a command prompt with parameters" on page 62.

For the procedure for running the silent installation or uninstallation using SMS, see "Running the silent installation with SMS" on page 63.

Uninstalling the monitoring agent on Windows systems

To uninstall the monitoring agent, complete the following steps:

1. Select **Start** > **Control Panel** > **Add or Remove Programs**.
2. Double-click **IBM Tivoli Monitoring**.
3. Choose **Modify** and click **Next**.
4. Deselect the monitoring agent to uninstall it. The uninstallation wizard is started.
5. Follow the on-screen prompts to complete the uninstallation.

After you uninstall the ITCAM for SOA SDMS agent, you must manually remove offline nodes from the Navigator in the Tivoli Enterprise Portal. For more information, see "Removing ITCAM for SOA SDMS agent node from the Navigator view."

Removing ITCAM for SOA SDMS agent node from the Navigator view

Use the Managed System Status workspace in the Tivoli Enterprise Portal to remove ITCAM for SOA SDMS agent nodes from the Navigator view.

The Enterprise Navigator has a Managed System Status workspace that you can use to check for any offline managed systems and remove them from the Navigator view.

To remove an offline ITCAM for SOA SDMS agent node from the Tivoli Enterprise Portal, complete the following steps:

1. From the Navigator view, right-click the Enterprise node and select **Workspace** > **Managed Systems Status**. The Managed System Status workspace is displayed.
2. Search for offline ITCAM for SOA SDMS agent nodes. The nodes are named *host_name*:S4 and have a status of ***OFFLINE**.
3. Right-click all offline ITCAM for SOA SDMS agent nodes and select **Clear offline entry** to remove them.
4. Click **Yes** on the confirmation dialog to remove the nodes.
5. A Navigator update pending indicator is displayed in the Tivoli Enterprise Portal. Collapse and expand the Navigator tree to verify that all nodes are removed.

Installing and uninstalling language support

To enable full support for a language, you must install the Language Pack on the monitoring agent host and all hosts where the monitoring agent support files are installed (Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and all Tivoli Enterprise Portal desktop clients).

If you no longer want to use a language, uninstall the language pack for the language.

To install or uninstall language support, follow the procedures in "Installing and uninstalling language support" on page 75. When prompted for an agent to install or uninstall language support for, select **ITCAM for SOA SDMS Agent**.

Remember: This procedure assumes that language support for Tivoli Monitoring is already installed. If not, see the *IBM Tivoli Monitoring: Installation and Setup Guide* and install the base language support for Tivoli Monitoring before you install language support for the monitoring agent.

Installing and configuring ITCAM for SOA SDMS agent on Linux and UNIX systems

Before you install the ITCAM for SOA SDMS agent version 7.2 Fix Pack 1, review the software requirements for the agent in "Required software" on page 15.

If a previous version of the ITCAM for SOA SDMS agent is installed, you must uninstall this version and reinstall ITCAM for SOA SDMS agent version 7.2 Fix Pack 1. To uninstall the ITCAM for SOA SDMS agent, complete the procedure in "Uninstalling the monitoring agent on Linux and UNIX systems" on page 250.

When you uninstall the ITCAM for SOA SDMS agent, application support files for the agent are not uninstalled from Tivoli Monitoring. When you reinstall application support files for the agent, you might see a message that indicates that the ITCAM for SOA SDMS agent is already installed. You can continue to install the agent.

Permissions for installing the ITCAM for SOA SDMS monitoring agent

If you have multiple Tivoli Monitoring components (including multiple monitoring agents) installed on the same computer, you should install all of the agents using the same user. (The only exception is the portal server which must be installed as root.)

If you do not want to install Tivoli Monitoring components, including the monitoring agents, as root on Linux and UNIX, create a user on the computer where you plan to install the Tivoli Monitoring components and use it to install all Tivoli Monitoring-related components (except the portal server) on that computer. For more information about creating the non-root user, see the *Create an IBM Tivoli account for installing and maintaining the installation directory* section of the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Enabling application support on the monitoring server, portal server, and desktop client

To ensure the ITCAM for SOA SDMS agent works within your Tivoli Monitoring infrastructure, application support files must be distributed to the Tivoli Monitoring components.

Application support files are automatically installed and enabled on the monitoring servers and the portal server, if the ITCAM for SOA SDMS agent and the monitoring servers are enabled for self-description. ITCAM for SOA SDMS agent is enabled by default for self-description. For more information, see “Enabling application support through self-description.”

If the agent and the Tivoli Monitoring components are not enabled for self-description, you must manually install application support files on the Tivoli Monitoring components. For more information, see “Installing and enabling application support manually before you install the agent” on page 240.

Enabling application support through self-description

When the ITCAM for SOA SDMS agent is installed and the monitoring servers and portal server are enabled for self-description, application support files are automatically installed on the monitoring servers and the portal server without the need to recycle the portal server and the monitoring server. Application support files must be installed manually on the portal client.

To verify that the application support files are installed, complete the following steps:

1. Open a command-line window and navigate to the Tivoli Monitoring installation bin directory.
2. Issue the `./cinfo` command.
3. Type 1 to see the list of applications support files that are installed.

The output lists the application support files that are installed. For example:

```
s4      Monitoring Agent for ITCAM for SOA SDMS
         aix523  Version: 07.20.01.00
         tms     Version: 07.20.01.00
         tps     Version: 07.20.01.00
         tpw     Version: 07.20.01.00
```

The self-describing agent feature is disabled by default on the hub monitoring server. The procedure for enabling self-description on the hub monitoring server is documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing and enabling application support manually before you install the agent

The following procedures refer to adding application support when the Tivoli Monitoring components are installed on a separate computer system to the monitoring agent. If the ITCAM for SOA SDMS agent and the Tivoli Monitoring components are on the same computer system, support files are installed when you install the agent.

When all of the Tivoli Monitoring components are installed on the same computer system, support files for each of the monitoring components must be installed at the same time.

When you manually install application support on your Tivoli Enterprise Monitoring Server, you must be logged in as the user who installed the Tivoli Enterprise Monitoring Server.

The Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and the Tivoli Enterprise Portal must be stopped before you install the application support files.

To install application support for the ITCAM for SOA agent and the ITCAM for SOA SDMS agent, complete the following steps:

1. Close the Manage Tivoli Enterprise Monitoring Services utility if it is open.
2. Mount the ITCAM for SOA SDMS installation media at the location you choose for the local system, following the standard procedures for the operating system.
3. From the root directory of the installation media, navigate to the `KS4` directory and extract the archive file for the ITCAM for SOA SDMS agent.
4. Navigate to the *`KS4_extract_folder`* directory and enter the following command to start the installation program: `./install.sh`.
5. When prompted for the Tivoli Monitoring home directory, press Enter to accept the default (`/opt/IBM/ITM`) or type the full path to the installation directory that you used. You are presented with the prompt `Ok to use`. Enter 1 and press Enter to confirm that the specified home directory can be used.
6. The following prompt is displayed:

   ```
   Select one of the following:
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS).
   3) Install TEMS support for remote seeding
   4) Exit install.
   Please enter a valid number:
   ```

7. Type 1 to start the installation and press Enter.
8. The software license agreement is displayed after the initialization. Enter 1 to accept the agreement and press Enter.
9. A numbered list of available operating systems and installation components is displayed:

   ```
   Product packages are available for the following operating systems and
   component support categories:
    1) IBM Tivoli Monitoring components for this operating system
    2) Tivoli Enterprise Portal Browser Client support
   ```

```
  3) Tivoli Enterprise Portal Desktop Client support
  4) Tivoli Enterprise Portal Server support
  5) Tivoli Enterprise Monitoring Server support
```

10. Type 5 to install application support for the monitoring server and press Enter.
11. Type 1 to confirm and press Enter.
12. The list of the components that are available for the installation of application support for the monitoring server is displayed. For example:

    ```
    The following application supports are available for installation:

    1) Monitoring Agent for ITCAM for SOA SDMS V07.20.01.00
    2) all of the above.
    ```

13. Enter the number that represents all components and press Enter.
14. Type 1 to confirm the installation of application support for the monitoring server. The installation begins.
15. When all of the components are installed, you are asked whether you want to install components for a different operating system. For example,

    ```
    Do you want to install additional products or product support
    packages [ 1=Yes, 2=No ; default is "2" ] ?
    ```

    Enter 1 to install application support for additional components.
16. The numbered list of available operating systems and installation components is displayed. Type 4 to install application support for the portal server and press Enter.
17. Type 1 to confirm and press Enter.
18. The list of the components that are available for the installation of application support for the portal server is displayed.
19. Enter the number that represents all components and press Enter.
20. Type 1 to confirm the installation of application support for the portal server. The installation begins.
21. When all of the components are installed, you are prompted to install components for a different operating system.
    Enter 1 to install application support for additional components.
22. The numbered list of available operating systems and installation components is displayed. Type 2 to install application support for the browser client or type 3 to install application support for the desktop client and press Enter.
23. Type 1 to confirm and press Enter.
24. The list of the components available for the installation of application support for the browser is displayed.
25. Enter the number that represents all components and press Enter.
26. Type 1 to confirm the installation of application support for the portal server. The installation begins.
27. When all of the components are installed, you are prompted to install components for a different operating system. Type 2 to confirm that no additional components are to be installed and press Enter.
28. When the installation program completes, you see a message that indicates that the application support files are installed:

    ```
    Following Tivoli Enterprise Monitoring Server product support were installed:
      *) Monitoring Agent for ITCAM for SOA SDMS
    Note: This operation causes the monitoring server to restart.
    ```

29. You are prompted to seed application support files on the monitoring server:

    ```
    Do you want to seed product support on the Tivoli Enterprise Monitoring Server?
    [ 1=Yes, 2=No ; defualt is "1" } ?
    ```

Type 1 to seed product support files.

30. You are prompted to add the default managed system groups when you process the application-support files:

    ```
    Choose one of the following options to add or update the situation
    distribution definition to include the default managed
    system groups:

     1) ALL - This option adds the default managed
    system groups to all the applicable situations.
    Note that not all situations have the
    default managed group setting. For some,
    you might need to manually define the distribution in the Tivoli
    Enterprise Portal due to the specific content
     of the agent support package.
     2) NONE - The default managed system group is not added to any situation.
    ```

    The *All* selection provides an option to add the default managed systems group to all applicable situations. Enter 1 to add the default managed system groups to all applicable situations and press Enter.

31. The installation program completes the installation and exits.
32. Reconfigure the portal server and the browser client to enable application support. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd config -A cq
    ```

    At any prompts, press Enter to accept the default values.

33. Restart the portal server. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd agent start cq
    ```

34. Reconfigure the desktop client to enable application support. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd config –A cj
    ```

    At any prompts, press Enter to accept the default values.

35. Restart the desktop client. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd agent start cj
    ```

36. Start the monitoring server. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd server start tems_name
    ```

37. Activate application support on the monitoring server. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd support -t tems_name d4
    ```

38. Stop the monitoring server. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd server stop tems_name
    ```

39. Restart the monitoring server to enable application support. Run the following command from the *ITM_HOME*/bin directory:

    ```
    ./itmcmd server start tems_name
    ```

Installing the ITCAM for SOA SDMS agent on Linux or UNIX systems

Complete the following procedure to install and configure the ITCAM for SOA SDMS agent on Linux or UNIX systems.

Before you begin

This installation of the ITCAM for SOA SDMS agent is based on the following assumptions:

- You installed or upgraded your Tivoli Monitoring environment to one of the minimum supported levels (see "Software and hardware prerequisites" on page 15).
- You already installed ITCAM for SOA SDMS application support for the Tivoli Monitoring components. For more information about installing application support, see "Enabling application support on the monitoring server, portal server, and desktop client" on page 239. If your IBM Tivoli Monitoring components are installed on the same computer systems as your application server runtime environment, application support can be installed during the installation of the monitoring agent.

The appropriate level of the Tivoli Enterprise Management Agent Framework is installed when the monitoring agent is installed.

About this task

The ITCAM for SOA SDMS agent can remotely query SDMS data, so you can install the agent on a separate system from the Tivoli Enterprise Portal Server.

Procedure

1. In the directory where you extracted the installation files for the ITCAM for SOA SDMS agent, run the following command: **`./install.sh`**
2. When prompted for the home directory, press Enter to accept the default directory (`/opt/IBM/ITM`) or type the full path to a different directory.

   Note: You must not specify the path of the directory that contains **`./install.sh`** as your home directory. On certain platforms, this can cause the plug-in JAR files to overwrite themselves and become zero length files. The installation fails as a result.
3. If the installation directory does not exist, you are asked if you want to create it. Type `y` to create this directory and press Enter.
4. The following prompt is displayed:

   ```
   Select one of the following:
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS).
   3) Install TEMS support for remote seeding
   4) Exit install.
   Please enter a valid number:
   ```

   Type 1 to start the installation.
5. The software license agreement is displayed. Type 1 to accept the agreement and press Enter.
6. Type a 32 character encryption key and press Enter. This key must be the same as the key that was used during the installation of the monitoring server to which this monitoring agent connects.
7. A numbered list of available operating systems is displayed. Type 1 to install the IBM Tivoli Monitoring support for your current operating system. Press Enter. A numbered list of available components is displayed.
8. Type the number that corresponds to the agent that you want to install. Press Enter. A list of the components to be installed is displayed.

9. Type 1 to confirm the installation. The installation begins.
10. After all of the components are installed, you are asked whether you want to install additional products or product support packages. Type 2 and press Enter.
11. If your IBM Tivoli Monitoring environment is not already secured, you are prompted to specify whether you want to secure it. The product installation process creates most of directories and files with world write permissions. IBM Tivoli Monitoring provides the **secureMain** utility to help you keep the monitoring environment secure. You can secure your installation now, or manually execute the **secureMain** utility later. For more information, see Appendix G, "Securing your IBM Tivoli Monitoring installation on Linux or UNIX systems", in the *IBM Tivoli Monitoring Installation guide*

Configure the ITCAM for SOA SDMS agent from the command line

If you plan to view Business Process Management monitoring data in SmartCloud Application Performance Management UI, you must configure the ITCAM for SOA SDMS agent. You can configure the agent in command line mode.

About this task

Use the following procedure to configure the ITCAM for SOA SDMS agent in command line mode:

Procedure

1. Navigate to the Tivoli Monitoring installation `bin` directory.
2. Run the following command: **`./itmcmd config -A s4`**
3. When you are asked if you want to edit the "Monitoring Agent for ITCAM for SOA SDMS" settings, press Enter.
4. When you are presented with the configuration parameters for connecting to the SOA Domain Management Server that are described in table Table 33, review the details and press Enter.

Table 33. TEPS SDMS Connection Information

Field	**Description**
`TEPS (SDMS) Server Hostname`	Host name of the Tivoli Enterprise Portal Server in which the SOA Domain Management Server is installed. The default value is localhost.
`User ID (e.g. sysadmin)`	User ID that is used to connect to SOA Domain Management Server, for example, `sysadmin`.
`Password`	Password for the user ID that is used to connect to SOA Domain Management Server.
`Background Collection Interval (in seconds)`	Background collection interval in seconds for data from SOA Domain Management Server. If you enter a value equal to or less than 0, the agent reverts to the default collection interval of 300 seconds.

Table 33. TEPS SDMS Connection Information (continued)

Field	Description
Java_home	The path to where an IBM Java Runtime Environment (JRE) is installed. By default, the Java_home parameter is not set. If you encounter problems with the default JRE that is used by the agent, you can specify a value for Java_home. If you set a value for Java_home, you must specify the location of an IBM JRE, Java version 6 or later. The ITCAM for SOA SDMS agent looks for the Java executable in the directory *JAVA_HOME*/bin.

5. Enter the Tivoli Enterprise Portal Server host name when you are prompted for TEPS SDMS Server Hostname, and press Enter.
6. Enter the user name and password for connecting to the Tivoli Enterprise Portal Server, and press Enter. Retype the password.
7. Enter the background collection interval in seconds, and press Enter.
8. Enter the background collection interval in seconds, and press Enter.
9. Press Enter when you are asked if the agent connects to a monitoring server.
10. Press Enter when you are asked to specify the Java home location.

    Tip: If you set a value for `Java_home` and you want to clear its value, enter a space when you are prompted for the value. Otherwise, when you press **Enter**, you retain the value that is currently set.
11. Enter the host name for the monitoring server.
12. Type the protocol that you want to use to communicate with the monitoring server. There are four choices available: `ip`, `sna`, `ip.pipe`, or `ip.spipe`. Press Enter to accept the default protocol (`ip.pipe`).
13. If you want to set up a backup protocol, enter that protocol and press Enter. You can specify up to three methods for communication. If the method you specify as protocol 1 fails, protocol 2 is used. If protocol 2 fails, protocol 3 is used.
14. Complete the fields for the protocols that you specified when prompted:

Table 34. IP, IP.PIPE, IP.SPIPE, and SNA field descriptions

Field	Description
IP.UDP Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port # or Port Pools	The listening port for the hub monitoring server. The default number is 1918.
IP.PIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.
Port Number	The listening port for the monitoring server. The default number is 1918.
IP.SPIPE Settings	
Hostname or IP Address	The host name or IP address for the hub monitoring server.

Table 34. IP, IP.PIPE, IP.SPIPE, and SNA field descriptions (continued)

Field	Description
Port number	The listening port for the hub monitoring server. The default value is 3660.
SNA Settings	
Network Name	The SNA network identifier for your location.
LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
LU 6.2 LOGMODE	The name of the LU6.2 LOGMODE. The default value is `CANCTDCS`.
TP Name	The transaction program name for the monitoring server.
Local LU Alias	Local LU Alias

15. You are prompted for the name of the `KDC_PARTITION`. If your site is using address translation, you must create a partition file. Partition IDs are specified using the `KDC_PARTITION` environment variable. Press Enter to skip this step. For more information about address translation, see "Appendix C: Firewalls" in the *IBM Tivoli Monitoring Installation and Setup Guide*.
16. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default value is `no`.
17. Press Enter to accept the default for the Optional Primary Network Name (none).

Configuring the ITCAM for SOA SDMS agent using a GUI

If you plan to view Business Process Management monitoring data in SmartCloud Application Performance Management UI, you must configure the ITCAM for SOA SDMS agent. You can configure the agent using a GUI.

About this task

Use the following procedure to configure the connection to the monitoring server:

Procedure

1. Navigate to the Tivoli Monitoring installation `bin` directory.
2. Run the following command: **`./itmcmd manage`** The Manage Tivoli Enterprise Monitoring Services window is displayed.
3. Select the ITCAM for SOA SDMS node. Right click it, and select **Configure**. The Configure Monitoring Agent for ITCAM for SOA SDMS window is displayed.
4. You are presented with the configuration parameters in table Table 35 for connecting to the SOA Domain Management Server. Modify the default values, as required.

Table 35. TEPS SDMS Connection Information

Field	Description
`TEPS (SDMS) Server Hostname`	Host name of the Tivoli Enterprise Portal Server in which the SOA Domain Management Server is installed. The default value is localhost.
`User ID (e.g. sysadmin)`	User ID that is used to connect to SOA Domain Management Server, for example, `sysadmin`.

Table 35. TEPS SDMS Connection Information (continued)

Field	Description
Password	Password for the user ID that is used to connect to SOA Domain Management Server.
Background Collection Interval (in seconds)	Background collection interval in seconds for data from SOA Domain Management Server. If you enter a value equal to or less than 0, the agent reverts to the default collection interval of 300 seconds.
Java_home	The path to where an IBM Java Runtime Environment (JRE) is installed. By default, the Java_home parameter is not set. If you encounter problems with the default JRE that is used by the agent, you can specify a value for Java_home. If you set a value for Java_home, you must specify the location of an IBM JRE, Java version 6 or later. The ITCAM for SOA SDMS agent looks for the Java executable in the directory *JAVA_HOME*/bin.

5. After you specify the configuration parameters for the ITCAM for SOA SDMS agent, click **OK**. The TEMS Connection window is displayed.
6. Clear the **No TEMS** check box.
7. Enter the Tivoli Enterprise Monitoring Server (TEMS) host name, and select the protocol for connecting with the Tivoli Enterprise Monitoring Server. If the connection must pass-through a firewall with address translation, select IP.PIPE, select the Use Address Translation check box, and set the port to 1918.
8. Specify protocol parameters and, if necessary the secondary protocols and secondary Tivoli Enterprise Monitoring Server host. For more information, see *IBM Tivoli Monitoring: Installation and Setup Guide* for details.
9. Click **Save**.

Silent installation on Linux and UNIX systems

In addition to installing the ITCAM for SOA SDMS agent interactively, the installer supports a silent mode. In this mode, no user interaction is required for an installation or uninstallation. Instead, the parameters are taken from a *response* file. You can install and uninstall the ITCAM for SOA SDMS agent and install application support files in silent mode.

Response files have a text format. You can create a response file that is based on one of the samples that are provided on the installation DVD or image.

You can also create a response file during installation, modify it if necessary, and then use it for a silent installation. In this way, you can reproduce similar configuration many times, for example, on different hosts.

Installing the ITCAM for SOA SDMS agent with a response file

You can use the installer to install ITCAM for SOA SDMS agent in silent mode. To install the agent in silent mode, modify the sample files that are on the installation DVD or image, and then run the installer on the command line.

The silent_install.txt sample response file specifies the installation parameters for installing the ITCAM for SOA agent and its application support files.

Before you complete a silent installation, edit the `silent_install.txt` file to indicate that you want to install.

To install ITCAM for SOA SDMS agent in silent mode, complete the following procedure:

1. In the top-level directory of the ITCAM for SOA installation DVD or image, locate the `silent_install.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify the following property, if necessary.

Table 36. ITCAM for SOA installation response file properties

Parameter	Definition
INSTALL_ENCRYPTION_KEY	Required. The data encryption key that is used to encrypt the data that is sent between systems. This key must be the same for all components in your Tivoli Monitoring environment.
INSTALL_PRODUCT=s4	Required. The product codes of the products to be installed. The product code of the ITCAM for SOA SDMS agent is `s4`.
INSTALL_PRODUCT_TMS=all	Uncomment this line to install application support for the monitoring server.
INSTALL_PRODUCT_TPS=all	Uncomment this line to install application support for the portal server.
INSTALL_PRODUCT_TPW=all	Uncomment this line to install application support for the portal browser client.
INSTALL_PRODUCT_TPD=all	Uncomment this line to install application support for the portal desktop client.
SEED_TEMS_SUPPORTS	If you are installing application support for the monitoring server, uncomment this line to seed application support to the monitoring server.
DEFAULT_DISTRIBUTION_LIST	If you are seeding application support on the monitoring server, specify which default distribution lists to upgrade. Valid values are ALL, NEW, or NONE. For more information about these values, see the comments in the `silent_install.txt` file.
SKIP_SDA_CHECK	Specify a value of "YES" to force agent seeding to occur. For more information about this value, see the comments in the `silent_install.txt` file.

4. Save the edited copy in a work directory, for example, as `/tmp/silent.txt`.
5. Run the following command to install ITCAM for SOA SDMS agent:

```
./install.sh -q -h install_dir -p response_file
```

Where:

install_dir
Identifies the installation location for the IBM Tivoli Monitoring component. The default installation location is `/opt/IBM/ITM`.

response_file
Identifies the response file that you edited to specify the installation parameters. Specify the absolute path to this file.

For example:

```
./install.sh -q -h /opt/ibm/itm -p /tmp/silent_install.txt
```

The sample `silent_install.txt` file presents all of the parameters that are required for the ITCAM for SOA SDMS agent and its support files. The file contains comments that explain each of the options.

Configuring the ITCAM for SOA SDMS agent with a response file

You can configure the ITCAM for SOA SDMS agent in silent mode. Prepare the response file by modifying a sample that was provided with the agent.

The sample response file, `silent_config.txt`, is in the top-level directory on the installation DVD or image.

To complete a configuration task, you must prepare a response file, and then start the configuration utility

Preparing a response file

To prepare a response file for configuring the agent, complete the following procedure:

1. On the ITCAM for SOA installation DVD, in the top-level directory, locate the `silent_config.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify the follow properties, if necessary:

Table 37. ITCAM for SOA installation response file properties

Parameter	Definition
KS4_SERVER_NAME	The host name of the Tivoli Enterprise Portal Server in which the SOA Domain Management Server is installed.
KS4_USER	User ID that is used to connect to SOA Domain Management Server, for example, `sysadmin`.
KS4_PASSWORD	Password for the user ID that is being used to connect to SOA Domain Management Server.
KS4_COLLECTION_INTERVAL	Background collection interval in seconds for data from SOA Domain Management Server. If you enter a value equal to or less than 0, the agent reverts to the default collection interval of 300 seconds.
KS4_JAVA_HOME	The path to where an IBM Java Runtime Environment (JRE) is installed. By default, the `Java_home` parameter is not set. If you encounter problems with the default JRE that is used by the agent, you can specify a value for `Java_home`. If you set a value for `Java_home`, you must specify the location of an IBM JRE, Java version 6 or later. The ITCAM for SOA SDMS agent looks for the Java executable in the directory *`JAVA_HOME`*`/bin`.

   For information about configuring the connection from the agent to the monitoring server, see the comments in the `silent_config.txt` sample response file.
4. Save the edited copy in a work directory, for example, as `/tmp/silent.txt`.

Running the Configuration utility in silent mode

After you prepare the response file for a configuration task, run the configuration utility, specifying the path and name for the response file. Complete the following procedure:

1. Change to the `ITM_home/bin` directory.
2. Start the configuration utility as follows. Specify the parameters in the exact order shown:

   ```
   itmcmd config -A -p response_file_name s4
   ```

   Where *response_file_name* is the name of the response file that you prepared (with full path). For example:

   ```
   itmcmd config -A -p /tmp/silent.txt s4
   ```

Performing a silent uninstallation

To uninstall the ITCAM for SOA SDMS agent in silent mode :

1. Change to the *ITM_home*/`bin` directory.
2. Run the following command:

   ```
   ./uninstall.sh -f s4 platform_code
   ```

   Where:

   -f Forces delete, suppressing confirmation messages and prompts.

   s4 Is the 2-letter code for the agent to be uninstalled.

   Platform
   Is the platform code for the product. To determine the platform code for your platform, see "Determining the *platform* value in directory paths" on page xvii

For more information about installing Tivoli Monitoring in silent mode, see "Appendix B. Performing a silent installation of IBM Tivoli Monitoring" in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Uninstalling the monitoring agent on Linux and UNIX systems

Uninstall the monitoring agent on supported Linux and UNIX operating systems by navigating to *ITM_Home*/`bin` folder and running the **`./uninstall.sh`** command. (For information about resolving directory path variables, see "Resolving directory path variables" on page xvi). Follow the on-screen prompts to complete the uninstallation.

After you uninstall the ITCAM for SOA SDMS agent, you must manually remove offline nodes from the Navigator in the Tivoli Enterprise Portal. For more information, see "Removing ITCAM for SOA SDMS agent node from the Navigator view" on page 237.

Installing and uninstalling language support

To enable full support for a language, you must install the Language Pack on the monitoring agent host and all hosts where the monitoring agent support files are installed (Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and all Tivoli Enterprise Portal desktop clients).

If you no longer want to use a language, uninstall the language pack for the language.

To install or uninstall language support, follow the procedures in "Installing and uninstalling language support" on page 108. When prompted for an agent to install or uninstall language support for, select **ITCAM for SOA SDMS Agent**.

Remember: This procedure assumes that language support for Tivoli Monitoring is already installed. If not, see the *IBM Tivoli Monitoring: Installation and Setup Guide* and install the base language support for Tivoli Monitoring before you install language support for the monitoring agent.

Configuring for remote deployment of the ITCAM for SOA SDMS agent

The ITCAM for SOA SDMS agents support the Tivoli Monitoring feature of remotely deploying the monitoring agent across your environment from a central location, the monitoring server.

Before you install the ITCAM for SOA SDMS monitoring agent on a remote system using Tivoli Enterprise Portal, the application support files (including browser client support files) must be enabled on the Tivoli Enterprise Portal Server, hub and remote Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal desktop clients.

Important: Remote deployment of ITCAM for SOA SDMS agent to a remote Windows 7 platform is not supported.

For more information about remote deployment in an IBM Tivoli Monitoring environment, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Adding installation bundles to the deployment depot

Before you can deploy a monitoring agent to a remote computer, you must add the operating system-specific monitoring agent bundle to the deployment depot. For example, if you are deploying monitoring agents to a Windows operating system, the Windows system bundle must be added to the deployment depot.

If you installed application support files for the monitoring server, you might have added the monitoring agents to the deployment depot during the installation. If not, you can add a monitoring agents bundle to the deployment depot at any time using the `tacmd addBundles` command.

For more information about this procedure, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Adding installation bundles to the deployment depot on Windows systems

To add a Windows system bundle to the deployment depot, complete the following steps:

1. Copy or mount the ITCAM for SOA SDMS agent installation images on the monitoring server host.
2. Change to the `ITM_HOME\bin` directory.
3. Use the following command to log in to the monitoring server:

   ```
   tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user and the password for the SYSADMIN user. For example:

   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```

4. (Optional) List the available bundles in the *path_to_Windows_image*\Windows\Deploy directory with the following command:

   ```
   tacmd listBundles -i path_to_Windows_image\Windows\Deploy
   ```

   You might receive a reply similar to the following message:

   ```
   Product Code : S4
   Deployable    : True
   Version      : 072001000
   Description  : Monitoring Agent for ITCAM for SOA SDMS
   Host Type    : WINNT
   Host Version : WINNT
   Prerequisites:
   ```

5. To add the installation bundle for Windows target hosts, enter this command:

   ```
   tacmd addBundles -i path_to_Windows_image\WINDOWS\Deploy -t s4
   ```

   The code s4 is the product code for the ITCAM for SOA SDMS agent. You might receive a reply similar to the following, where *Depot_dir* is the location where the deployment depot is located, for example, C:\IBM\ITM\CMS:

   ```
    KUICAB023I : Are you sure you want to add the following bundles to the
   <Depot_dir>\depot\ depot?

   Product Code : S3
   Deployable    : True
   Version      : 072001000
   Description  : Monitoring Agent for ITCAM for SOA SDMS
   Host Type    : WINNT
   Host Version : WINNT
   Prerequisites:
   KUICAB024I : Enter Y for yes or N for no:
   ```

   Enter Y to add the agent bundle to the deployment depot. Wait for the process to complete. A confirmation message is displayed when the bundle is added. You can use the **tacmd viewDepot** command to display the bundles that were added to the deployment depot.

Adding the installation bundles to the deployment depot on Linux and UNIX systems

To add a bundle for a Linux operating system to the deployment depot, complete the following steps:

1. Copy or mount the ITCAM for SOA monitoring agent installation images on the monitoring server host.
2. Change to the *ITM_HOME*/bin directory.

   For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
3. Run the following command to log in to the monitoring server:

   ```
   ./tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the Tivoli Monitoring SYSADMIN user and the password for the SYSADMIN user.

   For example:

   ```
   ./tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
4. (Optional) List the available bundles for the specific operating system in the *path_to_Linux_UNIX_image*/unix directory with the following command:

   ```
   ./tacmd listBundles -i path_to_Linux_UNIX_image/unix
   ```
5. To add the installation bundle for Linux or UNIX target hosts, enter this command:

   ```
   ./tacmd addBundles -i path_to_Linux_UNIX_image/unix -t s4
   ```

   The code s4 is the product code for the ITCAM for SOA SDMS agent.

Installing the ITCAM for SOA SDMS agent remotely with Tivoli Enterprise Portal

You can use the Tivoli Enterprise Portal to install the ITCAM for SOA SDMS agent remotely.

Before you install the ITCAM for SOA monitoring agent on a remote system, the application support files must be installed on the Tivoli Enterprise Portal Server (including the browser client support files), hub and remote Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal desktop clients.

Before you can install the ITCAM for SOA SDMS agent on a remote system, you must first deploy an OS monitoring agent to the remote system. See the *Tivoli Monitoring: Installation and Setup Guide* for details.

To install the ITCAM for SOA SDMS agent remotely with Tivoli Monitoring, complete the following procedure:

1. From the Navigator Physical view in the Tivoli Enterprise Portal, navigate to the computer where you want to install the monitoring agent.
2. Right-click the remote computer and select **Add Managed System**.
3. Select **Monitoring Agent for ITCAM for SOA SDMS** and click **OK**.
4. The New Managed System Configuration window is displayed. Accept the default to use the local system account or specify a valid account and password.
5. Click **Finish**. The agent installation process is started; you can track its progress in the Deployment Status workspace.

For more information about remotely installing an agent from the Tivoli Enterprise Portal, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing the ITCAM for SOA SDMS agent remotely from a command prompt

You can install the monitoring agent to a remote system from the command prompt of the monitoring server.

Before you can install the ITCAM for SOA SDMS agent on a remote system, you must first deploy an OS monitoring agent to the remote system. See the *Tivoli Monitoring: Installation and Setup Guide* for details

For details on using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

To install the monitoring agent with the command prompt, complete the following procedure on the monitoring server:

1. Change to the *ITM_HOME*\bin directory.

   For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.
2. Use the following command to log in to the monitoring server:

   ```
   tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user of Tivoli Monitoring and password. For example:

   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```

3. To install the ITCAM for SOA SDMS agent on a remote host, enter the **tacmd addSystem** command. Specify s4 as the product code for the ITCAM for SOA SDMS agent. Specify the node name. The name of the node includes the computer where the OS agent is installed and the product code for the OS agent:

   ```
   tacmd addSystem -t s4 -n node_name
   ```

   For example:

   ```
   tacmd addSystem -t s4 -n server1:NT
   ```

   Tip: Use the following command to discover the names of the nodes that are currently in use:

   ```
   tacmd listSystems -t UX NT LZ
   ```

4. If you want to monitor the remote deployment status, enter the following command:

   ```
   tacmd getDeployStatus
   ```

   The monitoring agent is installed.

For more information about remotely installing an agent from a command prompt, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

When the monitoring agent is successfully installed, it connects automatically to the monitoring server, and the portal desktop displays it.

Part 2. Configuring a data collector for WebSphere Application Server environments

After you run the installation program to install application support for the monitoring server, portal server, and desktop client, and after you install and configure the monitoring agent on the systems where services are to be monitored, you can install and configure the ITCAM Data Collector for WebSphere.

This part of the *IBM Tivoli Composite Application Manager for SOA Installation Guide* describes the procedures for configuring ITCAM Data Collector for WebSphere. It also describes the procedures for performing advanced configuration and customization of the data collector.

Chapter 7. Configuring data collection: WebSphere Application Server

Since the first release of ITCAM for SOA, monitoring of web services message traffic between services in a service-oriented architecture (SOA) in the IBM WebSphere Application Server runtime environment continues to expand and evolve. The initial focus on topology, pattern, and sequence discovery in WebSphere and IBM WebSphere Enterprise Service Bus environments was later broadened to include support for additional versions of IBM WebSphere Application Server and WebSphere Community Edition (CE). To provide a complete solution, additional capabilities were provided, including discovery and monitoring of web services, Service Component Architecture (SCA) components, and mediations hosted by IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server. ITCAM for SOA version 7.2 introduces the capability to monitor features of business applications of IBM Business Process Manager (BPM), such as BPMN processes, mediation flows, BPEL processes, human tasks, and adapters.

Support is also included for monitoring message traffic through the JAX-WS application programming interface in WebSphere Application Server version 7.0 and 8.0 and later versions. For a WebSphere environment, the monitoring method uses the AXIS2 implementation. The JAX-WS interface also supports SOAP version 1.2 requests and Web Services Description Language version 1.2. Filter controls are not supported.

Beginning with ITCAM for SOA version 7.2, managed SCA mediation primitives are no longer provided for insertion into mediation flow components of applications built with IBM WebSphere Integration Developer. The promotable properties of mediation primitives in IBM WebSphere Integration Developer provide a similar role.

A new data collector, ITCAM Data Collector for WebSphere, is introduced in ITCAM for SOA version 7.2 to monitor WebSphere Application Servers.

About the Service Component Architecture

IBM WebSphere Process Server and IBM WebSphere Enterprise Service Bus introduced a way to model services in an SOA environment, called the *Service Component Architecture* (SCA). SCA is designed to separate business logic from its implementation, so that you can focus on assembling an integrated application without knowing implementation details.

The Service Component Architecture is based on *SCA modules* and *SCA components*. A SCA module is made up of multiple SCA components. In ITCAM for SOA, SCA components are treated as Web Services Description Language (WSDL) service ports.

With additional support for IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server, ITCAM for SOA discovers information about messages that are flowing between SCA components.

ITCAM Data Collector for WebSphere is installed and application servers are configured once in the IBM WebSphere Process Server or IBM WebSphere Enterprise Service Bus environment. The data collector does not require each SCA application to be configured separately. When you deploy new SCA applications into your monitored environment, they are automatically monitored as well.

The SCA data collector supports both synchronous and asynchronous interactions that are flowing through the application server runtime environment.

Business Process Monitoring

ITCAM for SOA provides enhanced business monitoring support. ITCAM for SOA provides the capability to monitor the health of the applications on which business solutions are built. In addition to the service tracking available before version 7.2, ITCAM Data Collector for WebSphere in version 7.2 supports the monitoring of BPMN processes, mediation flows, BPEL processes, human tasks, and adapters.

ITCAM for SOA version 7.2 and ITCAM Agent for WebSphere Applications version 7.2 are both agents of ITCAM for Applications version 7.2. ITCAM for Applications delivers a BPM monitoring solution through the features of ITCAM for SOA and ITCAM Agent for WebSphere Applications. ITCAM for SOA monitors the health of applications that are running BPM processes. ITCAM Agent for WebSphere Applications monitors the health of the infrastructure resources of the BPM system. For an overview of the BPM monitoring solution provided by ITCAM for Applications, see the *IBM Tivoli Composite Application Manager for SOA BPM Monitoring Deployment Guide*.

To configure data collection for IBM BPM, complete the following steps:

1. Install the ITCAM for SOA monitoring agent and ITCAM Data Collector for WebSphere on the computer system where your WebSphere Application Server is installed.
2. Use the ITCAM Data Collector for WebSphere Configuration utility to integrate the data collector with the ITCAM for SOA monitoring agent and the ITCAM Agent for WebSphere Applications monitoring agent. Select the application server instances on which your business applications are running.
3. Install ITCAM Agent for WebSphere Applications on the same computer system. If you installed the same versions, release, and maintenance level of ITCAM Data Collector for WebSphere as part of the installation of ITCAM for SOA, reuse this data collector installation for ITCAM Agent for WebSphere Applications.

For more information about installing ITCAM Data Collector for WebSphere, see "Installing ITCAM for SOA 7.2, updating to 7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere" on page 261.

Considerations for installing and configuring IBM Business Process Manager

If you intend to monitor your business process applications through ITCAM for SOA, take the following into consideration when you install and configure IBM Business Process Manager (BPM):

1. To enable the monitoring of human tasks in ITCAM for SOA, you must enable common event infrastructure (CEI) logging for the Human Task Container and the Business Flow Manager in IBM BPM. CEI logging is disabled by default.

For more information about enabling CEI logging, see the “Enabling monitoring of business process and human task events” section in the IBM BPM information center.

Tip: Enabling audit logging or task history is not required.

2. To track all invocations of BPEL processes in ITCAM for SOA, you must enable SCA events in IBM BPM. To enable SCA events, follow the procedure in “Considerations for monitoring SCA events from IBM Business Process Manager Advanced” in the IBM BPM information center.
3. To update the namespace value associated with a BPEL process, you must deploy a new EAR file with the updated namespace. To ensure that the namespace value is updated on the UI for the BPEL process, complete the following steps:
   a. Stop the business process application using the WebSphere Integrated Solutions Console.
   b. Update the application with the new EAR file. The file contains the updated namespace value for the BPEL process.
   c. Restart the application.
4. To display metrics on Business Process Definition (BPD) nodes in the portal client when a SCA invokes a BPD process, the BPD must be in an active state. To activate a BPD in IBM Process Designer, complete the following steps:
   a. Log in to IBM Process Designer.
   b. Select the BPD.
   c. Right-click **Activate**.
5. Ensure that snapshots of process applications are deployed and activated on the Process Center. ITCAM for SOA does not monitor non-snapshot versions (for example, tip versions) of process applications.
6. Before you upgrade from IBM BPM version 7.5.1 fix pack 1 to version 8.0 or later, you must unconfigure ITCAM Data Collector for WebSphere. After you upgrade IBM BPM, reconfigure the data collector with the same settings. For more information about upgrading IBM BPM and configuring data collection, see “Configuring data collection for ITCAM for SOA when upgrading IBM BPM” on page 325.
7. The report request limit that is specified in the portal server environment file defines the normal limit of pending report requests to the portal server from a single client. In an IBM BPM environment, if many application servers are monitored on a single application server host, this limit might be exceeded. If you plan to configure data collection for multiple application servers, increase the report request limit from 50 to 100. For information about increasing the report request limit, see “Increasing the report request limit on the portal server” on page 172 on Windows systems or “Increasing the report request limit on the portal server” on page 226 on Linux or UNIX systems.
8. In the topology views in Tivoli Enterprise Portal, a link to the BPC Explorer can be made available in the flyover and Details window of a SCA human task or a BPEL component node. To make the link available, you must configure the BPC Explorer root URL. For more information about configuring the root URL, see “Configuring linking to the BPC Explorer” on page 319.

Restriction: In a BPEL to BPD invocation, the average response time metrics are not displayed on the link between the components in the Operational Flow workspaces in the Tivoli Enterprise Portal.

Common ITCAM Data Collector for WebSphere

ITCAM Data Collector for WebSphere is used by ITCAM for SOA for monitoring WebSphere Application Servers.

Products with ITCAM Data Collector for WebSphere

The data collector is shared with the following products:

- ITCAM Agent for WebSphere Applications version 7.2
- ITCAM for SOA version 7.2
- ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5
- ITCAM for Transactions version 7.3.0.1 and higher
- Application Performance Diagnostics Lite

Products with older versions of ITCAM Data Collector for WebSphere

The data collector components of the following products must be migrated to ITCAM Data Collector for WebSphere before you enable data collection for ITCAM Agent for WebSphere Applications version 7.2:

- Older versions of ITCAM Agent for WebSphere Applications, including:
  - ITCAM Agent for WebSphere Applications version 7.1
  - ITCAM for WebSphere version 6.1.0.4 or later
  - WebSphere Data Collector version 6.1.0.4 or later component of ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM for SOA version 7.1.1
- ITCAM for WebSphere Application Server version 7.2

You do not have to migrate the older version of the data collector if the data collector is configured for applications servers in a different WebSphere profile.

Earlier maintenance levels of ITCAM Data Collector for WebSphere

If an earlier maintenance level of ITCAM Data Collector for WebSphere is installed and configured for the same profile in which you want to enable data collection for ITCAM for SOA, you must update the maintenance level of the data collector. Use the ITCAM Data Collector for WebSphere Migration utility to update the data collector. When the data collector has been updated, you can enable data collection for ITCAM for SOA.

Configuring the data collector

In older versions of ITCAM for SOA, you install the data collector when installing the monitoring agent. Beginning with version 7.2, you install the monitoring agent first. After you install the monitoring agent, you install ITCAM Data Collector for WebSphere in a location that you specify. A configuration tool, the ITCAM Data Collector for WebSphere Configuration utility (`config.bat` on Windows systems or `config.sh` on Linux or UNIX systems), is used to configure the data collector.

With the configuration utility, you can integrate the data collector with the following components:

- ITCAM for SOA monitoring agent
- ITCAM Agent for WebSphere Applications monitoring agent
- ITCAM for Application Diagnostics Managing Server
- Tivoli Performance Viewer, available from the WebSphere administrative console
- Application Performance Diagnostics Lite
- ITCAM for Transactions Transactions Collector

New utilities are also provided for configuring the data collector. The utilities that you use and the configuration options that you choose in each utility depend on whether you are installing or upgrading the data collector and whether the same version or an older version of the data collector is configured for the same WebSphere profile in which you plan to enable data collection.

If you are performing an installation of ITCAM for SOA, refer to "Installing ITCAM for SOA 7.2, updating to 7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere" before installing the agent.

If you are performing an upgrade of ITCAM for SOA, refer to "Upgrading to V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere" on page 266 before upgrading the agent.

Data collector configuration utilities

ITCAM Data Collector for WebSphere is configured with the following configuration utilities:

- ITCAM Data Collector for WebSphere Configuration utility
- ITCAM Data Collector for WebSphere Reconfiguration utility
- ITCAM Data Collector for WebSphere Unconfiguration utility
- ITCAM Data Collector for WebSphere Migration utility

You can run each of the utilities in console mode or silent mode. To update the maintenance level of date collector, use the migration utility.

You might have to restart application servers for your configuration changes to take effect. At the end of the configuration task, the utilities provide a list of application servers that you must restart.

Installing ITCAM for SOA 7.2, updating to 7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere

To install ITCAM for SOA version 7.2 Fix Pack 1 in an environment where the agent is not already installed, complete the following steps:

1. Install the ITCAM for SOA 7.2 monitoring agent.
2. Update the monitoring agent to ITCAM for SOA version 7.2 Fix Pack 1.
3. Install and configure ITCAM Data Collector for WebSphere.

You might have installed an older version of data collector for another product and configured it for the same WebSphere profile in which you plan to configure data collection for ITCAM for SOA.

After you update the monitoring agent to version 7.2 Fix Pack 1, determine whether you have to install and configure or migrate the data collector:

- If the same version of the data collector is installed, the data collector installation and configuration is skipped.
- If an older version of the data collector is installed, you must migrate the data collector to ITCAM Data Collector for WebSphere.
- If an earlier maintenance level of the data collector is installed, you must migrate the data collector to the latest maintenance level of ITCAM Data Collector for WebSphere.

The following table provides a description of the scenarios under which ITCAM for SOA 7.2 Fix Pack 1 is installed. For a description of upgrade scenarios, see “Upgrading to V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere” on page 266.

Table 38. Pristine installation scenarios

Scenario	Where to find general procedure
Installing ITCAM for SOA V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere when the following conditions apply: • The data collector is not configured already for the same profile by the following products: – ITCAM Agent for WebSphere Applications version 7.2 or later – ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 or later – Application Performance Diagnostics Lite – ITCAM for Transactions version 7.3.0.1 or later • No older version of the data collector is configured for the same profile by the following products: – ITCAM for WebSphere version 6.1.0.4 or later – WebSphere Data Collector version 6.1.0.4 or later in ITCAM for Web Resources version 6.2.0.4 or later – ITCAM Agent for WebSphere Application version 7.1 in ITCAM for Application Diagnostics version 7.1 – ITCAM for WebSphere Application Server version 7.2	“Installing the data collector when neither the same version nor an older version is configured” on page 263

Table 38. Pristine installation scenarios (continued)

Scenario	Where to find general procedure
Installing ITCAM for SOA V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere when any of the following conditions apply: • An earlier maintenance level of the data collector is configured for the same profile by one of the following products: – ITCAM Agent for WebSphere Applications version 7.2 or later – ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 or later – Application Performance Diagnostics Lite – ITCAM for Transactions version 7.3.0.1 or later • An older version of the data collector is configured already for the same profile by one of the following products: – ITCAM for WebSphere version 6.1.0.4 or later – WebSphere Data Collector version 6.1.0.4 or later in ITCAM for Web Resources version 6.2.0.4 or later – ITCAM Agent for WebSphere Application version 7.1 in ITCAM for Application Diagnostics version 7.1 – ITCAM for WebSphere Application Server version 7.2	“Installing the data collector when an earlier maintenance level or an older version is configured” on page 264

Installing the data collector when neither the same version nor an older version is configured

The following procedure describes the steps for installing and configuring ITCAM for SOA V7.2 and updating to V7.2 Fix Pack 1 when neither the same version nor an older version of the ITCAM Data Collector for WebSphere is installed and configured for the same profile.

Before installing ITCAM for SOA V7.2, a number of prerequisites must be met and pre-installation tasks performed, for more information, see “Performing a pristine installation of ITCAM for SOA version 7.2 Fix Pack 1” on page 19.

Before updating to ITCAM for SOA V7.2 Fix Pack 1, a number of prerequisites must be met and pre-installation tasks performed, for more information, see “Updating to ITCAM for SOA version 7.2.0.1” on page 28.

To install ITCAM for SOA V7.2, update to V7.2 Fix Pack 1, and enable data collection for application servers, complete the following steps:

1. Install ITCAM for SOA V7.2 monitoring agent.
   (see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)
2. Update the ITCAM for SOA monitoring agent to V7.2 Fix Pack 1.
   a. Update the ITCAM for SOA monitoring agent to V7.2 Fix Pack 1.
   b. Install ITCAM Data Collector for WebSphere.

   (see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)

3. Enable data collection for ITCAM for SOA.
   Use the ITCAM Data Collector for WebSphere Configuration utility to complete the following steps:
   a. Integrate the data collector with the ITCAM for SOA monitoring agent.
   b. (Optional) Integrate the data collector with the following components:
      - ITCAM for Transactions
      - ITCAM Agent for WebSphere Applications monitoring agent
      - ITCAM for Application Diagnostics Managing Server
      - Tivoli Performance Viewer
      - Application Performance Diagnostics Lite.

      Remember: To integrate the data collector with an ITCAM for Application Diagnostics Managing Server, you must have installed and configured ITCAM for Application Diagnostics version 7.1.0.3.

   (See “Configuring ITCAM Data Collector for WebSphere” on page 274)
4. Restart the application servers as directed by the utility.
   (see “Restarting the application server” on page 351)
5. Complete any additional tasks to configure the ITCAM for SOA agent, for example, configuring topology support. For more information about the additional configuration tasks, see “Roadmap for updating from ITCAM for SOA version 7.2 to version 7.2.0.1” on page 30.

Installing the data collector when an earlier maintenance level or an older version is configured

The following procedure describes the steps for installing and configuring ITCAM for SOA V7.2 and updating to V7.2 Fix Pack 1 when an earlier maintenance level or other older versions of the ITCAM Data Collector for WebSphere are installed and configured for application servers within the same profile.

Before installing ITCAM for SOA V7.2, a number of prerequisites must be met and pre-installation tasks performed, for more information, see “Performing a pristine installation of ITCAM for SOA version 7.2 Fix Pack 1” on page 19.

Before updating to ITCAM for SOA V7.2 Fix Pack 1, a number of prerequisites must be met and pre-installation tasks performed, for more information, see “Updating to ITCAM for SOA version 7.2.0.1” on page 28.

To install ITCAM for SOA V7.2, update to V7.2 Fix Pack 1, and enable data collection for application servers, complete the following steps:

1. Install ITCAM for SOA V7.2 monitoring agent.
   (see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)
2. Update the ITCAM for SOA to V7.2 Fix Pack 1:
   a. Update the ITCAM for SOA monitoring agent.
   b. Install ITCAM Data Collector for WebSphere.

      Note: If an earlier version of ITCAM Agent for WebSphere Applications is installed on the computer system, do not specify the ITCAM Agent for WebSphere Applications home directory as the data collector home directory.

   c. When the installation is complete, the ITCAM Data Collector for WebSphere Configuration Utility starts automatically. Exit the utility.

   (see Chapter 2, "Installing or upgrading ITCAM for SOA on Windows systems," on page 35 or Chapter 3, "Installing ITCAM for SOA on Linux and UNIX systems," on page 77)

3. Migrate any older versions of the data collector. To migrate the data collector, complete the following steps:
   a. If an older version of the ITCAM Agent for WebSphere Applications is configured for the same profile, use the migration utility to migrate the data collector to ITCAM Data Collector for WebSphere for application server instances. After migration, the data collector communicates with the previous version of the monitoring agent or managing server, or both.

      If you later upgrade the ITCAM Agent for WebSphere Applications monitoring agent to version 7.2, you must reconfigure the data collector to connect to the 7.2 version of the ITCAM Agent for WebSphere Applications monitoring agent, which uses a different port to older versions of the monitoring agent.
   b. If ITCAM for WebSphere Application Server version 7.2 is configured for the same profile, use the migration utility to migrate its data collector to the ITCAM Data Collector for WebSphere for application server instances.
   c. If an earlier maintenance level of ITCAM Data Collector for WebSphere is installed by any of the following products, you must update the data collector:
      - ITCAM Agent for WebSphere Applications version 7.2 or later
      - ITCAM for WebSphere Application Server version 7.2 or later
      - Application Performance Diagnostics Lite

      Use the migration utility to migrate the data collector to use the latest maintenance level for one or more application server instances.

   Important: If multiple server instances are configured within the same WebSphere profile, you must migrate data collection for all server instances at the same time.
   (see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291)
4. Restart the application servers as directed by the utility.
   (see "Restarting the application server" on page 351)
5. Enable data collection for ITCAM for SOA.
   Run either the configuration or reconfiguration utility to reconfigure the data collector.

   To reconfigure the data collector, complete the following steps:
   a. Integrate the data collector with ITCAM for SOA monitoring agent.
   b. (Optional) Reconfigure the integration of the data collector with the following components:
      - ITCAM for Transactions
      - ITCAM Agent for WebSphere Applications monitoring agent
      - ITCAM for Application Diagnostics Managing Server
      - Tivoli Performance Viewer
      - Application Performance Diagnostics Lite

   (see "Reconfiguring ITCAM Data Collector for WebSphere" on page 284)

6. Restart the application servers as directed by the utility.
   (see "Restarting the application server" on page 351)
7. Complete any additional tasks to configure the ITCAM for SOA agent, for example, configuring topology support. For more information about the additional configuration tasks, see "Roadmap for updating from ITCAM for SOA version 7.2 to version 7.2.0.1" on page 30.

Upgrading to V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere

To upgrade to ITCAM for SOA version 7.2 Fix Pack 1 in an environment where ITCAM for SOA version 7.1.1 is installed, you complete the following steps:

1. Upgrade the monitoring agent to ITCAM for SOA version 7.2.
2. Update the monitoring agent to ITCAM for SOA version 7.2 Fix Pack 1.
3. Migrate ITCAM Data Collector for WebSphere.

When you upgrade the monitoring agent to ITCAM for SOA version 7.2, skip the installation of ITCAM Data Collector for WebSphere. Instead, when you update the monitoring agent to ITCAM for SOA version 7.2 Fix Pack 1, install the data collector and migrate any previous versions of the data collector.

You can migrate all application servers in a WebSphere profile to use the ITCAM Data Collector for WebSphere.

Alternatively, you can configure a subset of application servers to use the ITCAM Data Collector for WebSphere. All other application servers remain at version 7.1.1. At a later time, you can reconfigure the application servers to use the new data collector.

When you upgrade a subset of application servers, the following metric log files are produced:

- The ITCAM for SOA version 7.1.1 WebSphere Application Server data collector produces metric log files that are compatible with the ITCAM for SOA version 7.1.1 monitoring agent.
- The ITCAM Data Collector for WebSphere produces metric log files that are compatible with the ITCAM for SOA version 7.2 monitoring agent.

To avoid any confusion about whether an ITCAM for SOA 7.1.1 version of a metric log file is generated legitimately, stop the ITCAM for SOA version 7.1.1 data collector from producing metric log files. Use the **DisableDC_610** take action command on the portal server to stop data collection. After you upgrade the subset of application servers, use the **EnableDC_610** take action command to restart data collection.

Important: The ITCAM for SOA version 7.2 monitoring agent can consume metric files from an ITCAM for SOA version 7.1.1 WebSphere Application Server data collector and from ITCAM Data Collector for WebSphere.

Table 39 on page 267 provides a description of the scenarios under which ITCAM for SOA 7.2 Fix Pack 1 is upgraded.

Table 39. Upgrade scenarios

Scenario	Where to find the general procedure
Upgrading to ITCAM for SOA V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere when the following conditions apply: • The data collector is not configured already for the same profile by the following products: – ITCAM Agent for WebSphere Applications version 7.2 or later – ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 or later – Application Performance Diagnostics Lite – ITCAM for Transactions version 7.3.0.1 or later • No older version of the data collector is configured for the same profile by the following products: – ITCAM for WebSphere version 6.1.0.4 or later – WebSphere Data Collector version 6.1.0.4 or later in ITCAM for Web Resources version 6.2.0.4 or later – ITCAM Agent for WebSphere Application version 7.1 in ITCAM for Application Diagnostics version 7.1 – ITCAM for WebSphere Application Server version 7.2	"Migrating to ITCAM Data Collector for WebSphere when neither the same version nor an older version is configured by another product" on page 268
Upgrading to ITCAM for SOA V7.2, updating to V7.2 Fix Pack 1, and configuring ITCAM Data Collector for WebSphere when the following conditions apply: • An earlier maintenance level of the ITCAM Data Collector for WebSphere is configured for the same profile by one of the following products: – ITCAM Agent for WebSphere Applications version 7.2 or later – ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 or later – Application Performance Diagnostics Lite • An older version of ITCAM Data Collector for WebSphere is configured already for the same profile by one of the following products: – ITCAM for WebSphere version 6.1.0.4 or later – WebSphere Data Collector version 6.1.0.4 or later in ITCAM for Web Resources version 6.2.0.4 or later – ITCAM Agent for WebSphere Application version 7.1 in ITCAM for Application Diagnostics version 7.1 – ITCAM for WebSphere Application Server version 7.2	"Migrating to ITCAM Data Collector for WebSphere when an earlier maintenance level or another older version is configured" on page 269

Migrating to ITCAM Data Collector for WebSphere when neither the same version nor an older version is configured by another product

The following procedures describe the steps for upgrading to ITCAM for SOA version V7.2 and updating to V7.2 Fix Pack 1 when neither the same version nor an older version of the ITCAM Data Collector for WebSphere is installed and configured for the same profile by another product.

Before upgrading to ITCAM for SOA version 7.2, a number of prerequisites must be met and pre-installation tasks performed, for more information, see “Upgrading to ITCAM for SOA version 7.2” on page 23.

Before updating to ITCAM for SOA V7.2 Fix Pack 1, a number of prerequisites must be met and pre-installation tasks performed, for more information, see “Updating to ITCAM for SOA version 7.2.0.1” on page 28.

To upgrade to ITCAM for SOA V7.2, update to V7.2 Fix Pack 1, and enable data collection for application servers, complete the following steps:

1. If you are upgrading only a subset of application servers to version 7.2 Fix Pack 1, optionally deactivate data collection for the 7.1.1 version for the data collector using the **`DisableDC_610`** take action command. While deactivated, the 7.1.1 version of the data collector does not produce metric log files.
   For information about using the **`DisableDC_610`** command, see the *Take Action* commands section of the *IBM Tivoli Composite Application Manager for SOA User's Guide*.
2. If you are upgrading all application servers to version 7.2, disable data collection for the WebSphere Application Server and restart the WebSphere Application Server.
   (see “Before upgrading ITCAM for SOA” on page 24).
3. Upgrade the ITCAM for SOA monitoring agent to V7.2.
   (see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)
4. Update the ITCAM for SOA monitoring agent to V7.2 Fix Pack 1.
   (see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)
5. Install the ITCAM Data Collector for WebSphere.
   Do not select the *ITCAM4SOA_Home* directory used by the ITCAM for SOA version 7.1.1 installation. (see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)
6. When the installation is complete, the ITCAM Data Collector for WebSphere Configuration Utility starts automatically. Exit the utility.
7. Migrate the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector. To migrate the data collector using the migration utility, complete the following steps:
   a. Enable data collection for one or more application server.
   b. (Optional) Reconfigure the data collector. From the Summary section, configure the integration of the data collector with the following components:
      - ITCAM for Transactions

- ITCAM Agent for WebSphere Applications monitoring agent
- ITCAM for Application Diagnostics Managing Server
- Tivoli Performance Viewer
- IBM Application Performance Diagnostics

(see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 294)

8. Restart the application servers as directed by the utility.
   (see "Restarting the application server" on page 351)
9. If you deactivated the 7.1.1 version of the data collector in step 1 on page 268, activate the data collector using the **EnableDC_610** take action command.
   For information about using the **EnableDC_610** take action command, see the *Take Action* commands section of *IBM Tivoli Composite Application Manager for SOA User's Guide*.
10. Complete any additional tasks to configure the ITCAM for SOA agent, for example, configuring topology support. For more information about additional configuration tasks, see "Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1" on page 20.
11. When you have upgraded data collection for all application servers, optionally remove the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector. For information about removing the data collector, see "Removing ITCAM for SOA version 7.1.1 WebSphere Application Server data collector" on page 271.

Migrating to ITCAM Data Collector for WebSphere when an earlier maintenance level or another older version is configured

This following procedures describe the steps for upgrading to ITCAM for SOA V7.2 and updating to V7.2 Fix Pack 1 when either of the following conditions apply:

- An earlier maintenance level of the ITCAM Data Collector for WebSphere is installed by another product within the same WebSphere profile.
- Another older version of the ITCAM Data Collector for WebSphere is installed and configured for application servers within the same profile.

Before upgrading the ITCAM for SOA WebSphere Application Server data collector to version 7.2, refer to the "Upgrading to ITCAM for SOA version 7.2" on page 23 section for upgrade prerequisites that must be met and pre-upgrade tasks that must be performed before an upgrade of ITCAM for SOA.

To upgrade to ITCAM for SOA V7.2, update to V7.2 Fix Pack 1, and enable data collection for application servers, complete the following steps:

1. If you are upgrading only a subset of application servers to V7.2, optionally deactivate data collection for the 7.1.1 version for the data collector using the **DisableDC_610** take action command. While deactivated, the 7.1.1 version of the data collector does not produce metric log files.
   For information about using the **DisableDC_610** command, see the *Take Action* commands section of *IBM Tivoli Composite Application Manager for SOA User's Guide*.
2. If you are upgrading all application servers to version 7.2 Fix Pack 1, disable data collection for the WebSphere Application Server and restart the WebSphere Application Server.
   (see "Before upgrading ITCAM for SOA" on page 24).

3. Upgrade the ITCAM for SOA monitoring agent to V7.2.
   (see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)
4. Update the ITCAM for SOA monitoring agent to V7.2 Fix Pack 1.
   (see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)
5. Install the ITCAM Data Collector for WebSphere.
   Do not select the *ITCAM4SOA_Home* directory used by the ITCAM for SOA 7.1.1 installation. Do not select the data collector home directory used by any ITCAM for WebSphere 6.1.0.4 or later, WebSphere Data Collector 6.1.0.4 or later, or ITCAM Agent for WebSphere Applications 7.1 installations.(see Chapter 2, “Installing or upgrading ITCAM for SOA on Windows systems,” on page 35 or Chapter 3, “Installing ITCAM for SOA on Linux and UNIX systems,” on page 77)
6. When the installation is complete, the ITCAM Data Collector for WebSphere Configuration Utility starts automatically. Exit the utility.
7. Migrate the older versions of the data collector. To migrate the data collector using the migration utility, complete the following steps:
   a. If an older version of the ITCAM Agent for WebSphere Applications is configured for the same profile, use the migration utility to migrate the older version of the data collector to the ITCAM Data Collector for WebSphere for application server instances. The data collector communicates with the older version of the ITCAM Agent for WebSphere Applications monitoring agent.

      When you later upgrade the ITCAM Agent for WebSphere Applications monitoring agent to version 7.2, you must reconfigure the data collector to connect to the ITCAM Agent for WebSphere Applications version 7.2 monitoring agent. The monitoring agent in version 7.2 uses a different port to older versions of the monitoring agent.

      The ITCAM for SOA version 7.1.1 data collector is upgraded automatically as part of the migration of the older version of the ITCAM Agent for WebSphere Applications data collector.
   b. If ITCAM for WebSphere Application Server 7.2 is configured for the same profile, use the migration utility to migrate the ITCAM for WebSphere Application Server data collector to ITCAM Data Collector for WebSphere for application server instances.

      The ITCAM for SOA 7.1.1 data collector is upgraded automatically as part of the migration of the ITCAM for WebSphere Application Server data collector.
   c. If an earlier maintenance level of the ITCAM Data Collector for WebSphere is installed by any of the following products, you must update the data collector:
      - ITCAM Agent for WebSphere Applications version 7.2 or later
      - ITCAM for WebSphere Application Server version 7.2 or later
      - ITCAM for Transactions version 7.3.0.1 or later
      - IBM Application Performance Diagnostics

      Use the migration utility to migrate the data collector to use the latest maintenance level of the data collector for application server instances.

The ITCAM for SOA version 7.1.1 data collector is upgraded automatically as part of the migration of the older maintenance level of the ITCAM Data Collector for WebSphere.

(see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291)

8. Restart the application servers as directed by the utility.
   (see "Restarting the application server" on page 351)
9. Enable data collection for ITCAM for SOA.
   Run either the configuration or reconfiguration utility to reconfigure the data collector. With the utility, integrate the data collector with the ITCAM for SOA monitoring agent. Optionally, reconfigure the integration of the data collector with the following components:
   - ITCAM for Transactions
   - ITCAM Agent for WebSphere Applications monitoring agent
   - ITCAM for Application Diagnostics Managing Server
   - Tivoli Performance Viewer
   - IBM Application Performance Diagnostics

   (see "Reconfiguring ITCAM Data Collector for WebSphere" on page 284)
10. Restart the application servers as directed by the utility.
    (see "Restarting the application server" on page 351)
11. If you deactivated the 7.1.1 version of the data collector in step 1 on page 269, activate the data collector using the **EnableDC_610** take action command.
    For information about using the **EnableDC_610** take action command, see the *Take Action* commands section of *IBM Tivoli Composite Application Manager for SOA User's Guide*.
12. Complete any additional tasks to configure the ITCAM for SOA agent, for example, configuring topology support. For more information about the additional configuration tasks, see "Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1" on page 20.
13. When you have upgraded data collection for all application servers, optionally remove the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector. For information about removing the data collector, see "Removing ITCAM for SOA version 7.1.1 WebSphere Application Server data collector."

Removing ITCAM for SOA version 7.1.1 WebSphere Application Server data collector

When you have upgraded data collection for all application servers to ITCAM for SOA version 7.2, you can remove the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector. To manually remove the associated JAR files, complete the following steps:

1. Delete the `kd4*` files in the `WAS/lib/ext` directory on Windows systems or in the `WAS\lib\ext` on Linux and UNIX systems.
2. Delete the `com.ibm.management.soa.*` files in the `WAS/plugins` directory on Windows systems or in the `WAS\plugins` directory on Linux and UNIX systems.

Updating to V7.2 Fix Pack 1 and configuring ITCAM Data Collector for WebSphere

To update to ITCAM for SOA version 7.2 Fix Pack 1 in an environment where ITCAM for SOA version 7.2 is installed, you must update the monitoring agent to version 7.2 Fix Pack 1 and migrate the data collector to the latest maintenance level.

To update to ITCAM for SOA version 7.2 Fix Pack 1 and enable data collection for application servers, complete the following steps:

1. Update the ITCAM for SOA monitoring agent.
   (see Chapter 2, "Installing or upgrading ITCAM for SOA on Windows systems," on page 35 or Chapter 3, "Installing ITCAM for SOA on Linux and UNIX systems," on page 77)
2. When the installation is complete, the ITCAM Data Collector for WebSphere Configuration Utility starts automatically. Exit the utility.
3. Migrate the data collector to the latest maintenance level. To migrate the data collector using the migration utility, complete the following steps:
   a. Enable data collection for one or more application server.
   b. (Optional) Reconfigure the data collector. From the Summary section, configure the integration of the data collector with the following components:
      - ITCAM for Transactions
      - ITCAM Agent for WebSphere Applications monitoring agent
      - ITCAM for Application Diagnostics Managing Server
      - Tivoli Performance Viewer
      - IBM Application Performance Diagnostics

   (see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 294)
4. Restart the application servers as directed by the utility.
   (see "Restarting the application server" on page 351)
5. Complete any additional tasks to configure the ITCAM for SOA agent, for example, configuring topology support. For more information about additional configuration tasks, see "Roadmap for installing ITCAM for SOA version 7.2 Fix Pack 1" on page 20.

Communicating with ITCAM for Transactions

IBM Tivoli Composite Application Manager for Transactions (ITCAM for Transactions) is an IBM Tivoli Monitoring-based product that provides a unified, end-to-end transaction tracking solution for the IT Operations segment. ITCAM for Transactions tracks transactions within and among applications. It determines the time spent by a transaction in each application and, where possible, the time spent communicating between applications.

The ITCAM Data Collector for WebSphere supports integration with ITCAM for Transactions. When you enable support, the data collector provides request and transaction data to ITCAM for Transactions. Support is facilitated through the Transaction Tracking application programming interface (TTAPI). Once you install the data collector, you can configure support with the ITCAM Data Collector for WebSphere Configuration utility.

For details on configuring the data collector, see “Configuring the data collector interactively.” After you have installed and configured the data collector to support ITCAM for Transactions, you then need to perform some additional configuration. For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.

Permissions needed to configure data collection

When you configure ITCAM Data Collector for WebSphere to monitor instances of an application server, the user must have privileges (read, write, and execute) for the application server directory.

The user must have permission to execute scripts in the `DC_home\bin` directory on Windows systems or `DC_home/bin` on Linux or UNIX systems.

Run the configuration utilities using a Windows, Linux, or UNIX operating system user ID that owns the WebSphere Application Server profile that is being configured. If the WebSphere Application Server installer and profile owner do not map to the same Windows, Linux, or UNIX operating system user ID, follow the steps in the WebSphere Application Server information center on configuring the profile user. For more information, see the WebSphere Application Server information center.

If WebSphere global security is enabled, the configuration utilities prompt you for a WebSphere administrative user ID with login privileges to the wsadmin tool. Specify a user ID that is the primary administrative user. For more information, see the WebSphere Application Server information center.

Setting up user permissions for non-root users

It is important on Linux and UNIX operating systems that the user who installed the monitoring agent and the user who owns the application server environment are in the same group (for example, *itmusers*) if non-root users are used. For more information about setting up permissions, see “Permissions for installing, upgrading, or updating the monitoring agent” on page 83.

The WebSphere Application Server typically must be stopped and restarted for the data collection configuration to take effect.

Configuring the data collector interactively

There are a number of command-line configuration utilities to configure, reconfigure, unconfigure, and migrate ITCAM Data Collector for WebSphere.

The following table provides a description of the configuration tasks supported by the utilities.

Table 40. Configuration tasks

Configuration task	Where to find the procedure
Configure the data collector to monitor application server instances within a WebSphere Application Server profile. This configuration utility is started automatically when you install the monitoring agent.	“Configuring ITCAM Data Collector for WebSphere” on page 274

Table 40. Configuration tasks (continued)

Configuration task	Where to find the procedure
Modify the configuration of the data collector for application server instances that were already configured by the ITCAM Data Collector for WebSphere Configuration utility.	"Reconfiguring ITCAM Data Collector for WebSphere" on page 284
Unconfigure the data collector.	"Unconfiguring ITCAM Data Collector for WebSphere" on page 282
Migrate an older version of the data collector to ITCAM Data Collector for WebSphere or update the maintenance level of ITCAM Data Collector for WebSphere.	"Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291
Migrate the WebSphere Application Server data collector provided by ITCAM for SOA version 7.1.1 to ITCAM Data Collector for WebSphere.	"Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 294

Important: To change to a later maintenance level of ITCAM Agent for WebSphere Applications, use the migration utility (see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291).

Guidelines on which configuration utility to run

Use the following guidelines to determine whether to run the configuration or reconfiguration utility to configure application servers:

- If the application servers you plan to configure are not yet configured for data collection, use the configuration utility.

  If you run the configuration utility on any application servers that are already configured for data collection, your data collector configuration settings are overwritten.
- If the application servers that you plan to configure are already configured for data collection, use the reconfiguration utility to retain your existing data collector configuration settings.
- If some of the application servers you plan to configure are already configured and others are not yet configured, complete either of the following steps:
  - Use the configuration utility to configure the application servers. The data collection settings of the applications servers are overwritten.
  - Alternatively, run the configuration utility for the set of servers that have not yet been configured and run the reconfiguration utility for the servers that are already configured.

To apply different configuration settings to sets of application servers, run either utility for each set of servers separately.

Configuring ITCAM Data Collector for WebSphere

You must configure the data collector for each application server instance that you want to monitor.

The ITCAM Data Collector for WebSphere Configuration utility is a menu driven command-line utility for configuring ITCAM Data Collector for WebSphere.

If you are installing the data collector, the installer automatically launches the configuration utility.

Important: In an ITCAM for Application Diagnostics deployment, do not configure the data collector to monitor an instance of WebSphere Application Server that hosts the managing server visualization engine (MSVE). However, you can use the data collector to monitor any other WebSphere Application Server instances that are on the same node.

Remember: If you have already configured the data collector and you want to reconfigure it, start the ITCAM Data Collector for WebSphere Reconfiguration utility. Otherwise, the changes you made are lost.

To configure the data collector to monitor one or more server instances, complete the following procedure:

1. If you are installing the monitoring agent where the ITCAM Data Collector for WebSphere Configuration utility is started automatically by the installer, proceed to step 4. Otherwise, from the command line, navigate to the `DC_home\bin` directory on Windows systems or the `DC_home/bin` directory on Linux or UNIX systems.
2. Set the location of the Java home directory before you run the utility. For example:

   on Windows systems:

   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```

   on Linux or UNIX systems:

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```
3. Run the following command to start the configuration utility.

   On Windows systems:

   ```
   DC_home\bin\config.bat
   ```

   On Linux or UNIX systems:

   ```
   DC_home/bin/config.sh
   ```
4. The utility starts and displays the IP addresses of all network cards that are found on the local computer system. The utility prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```
5. Enter the number that corresponds to the IP address to use.

   The utility searches for WebSphere Application Server home directories on the computer system and prompts you to select a home directory:

   On Windows systems:

   ```
   List of WebSphere Application Server home directories discovered:
     1. C:\Program Files\IBM\WebSphere\AppServer
   Enter a number or enter the full path to a home directory
   [default is: 1]:
   ```

   On Linux or UNIX systems:

   ```
   List of WebSphere Application Server home directories discovered:
     1. /opt/IBM/WebSphere/AppServer
   Enter a number or enter the full path to a home directory
   [default is: 1]:
   ```
6. Enter the number that corresponds to a WebSphere Application Server home directory.

   The utility searches for all profiles under the specified home directory and prompts you to select a profile:

```
List of WebSphere profiles discovered:
  1. AppSrv01
Enter a number [default is: 1]:
```

7. Enter the number that corresponds to the WebSphere Application Server profile that you want to configure.

   The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile that you specified:

   ```
   WebSphere Global Security is enabled.
   ```

   If global security is not enabled, skip to step 9

8. The utility prompts you to specify whether to retrieve security settings from a client properties file:

   ```
   Do you want to retrieve security settings from a client properties file
   (soap.client.props or sas.client.props)?
   [1 - YES, 2 - NO] [default is: 2]:
   ```

   The data collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the Simple Object Access Protocol (SOAP) protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for an SOAP connection.

   Enter 1 to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 9. Otherwise, enter 2 to enter the user name and password.

   ```
   Enter WebSphere admin user name:
   Enter WebSphere admin user password:
   ```

9. The utility searches for all application server instances under the specified profile. The utility displays all servers that are not configured yet for data collection and all servers that are configured to use the current version of ITCAM Data Collector for WebSphere.

   The utility prompts you to select one or more application server instances from the list:

   ```
   Choose one or more servers to configure for data collection:
   Application servers not yet configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:
   ```

   Remember:

   - For a stand-alone environment, application server instances must be running during the configuration.
   - For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
   - Ensure that the application server instances that you select are the actual servers that host the applications or services that you want to monitor.

10. Enter the number that corresponds to the application server instance to configure for data collection or enter an asterisk (*) to configure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: `1,2,3`.

11. In the **Integration with ITCAM for SOA Agent** section, the utility provides an option for integrating the data collector with the ITCAM for SOA agent.

    ```
    Do you want to integrate with an ITCAM for SOA Agent? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    You must install and configure the ITCAM for SOA Agent and its application support files, and optionally configure topology support to complete the installation and configuration of the ITCAM for SOA agent. For more information about installing and configuring the ITCAM for SOA Agent, see *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

    Enter 1 to integrate the data collector with the ITCAM for SOA Agent. Otherwise, enter 2.

12. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with ITCAM Agent for WebSphere Applications.

    When configuring data collection for ITCAM Agent for WebSphere Applications, you can integrate the data collector with the ITCAM Agent for WebSphere Applications monitoring agent, or with the ITCAM for Application Diagnostics Managing Server, or with both.

    ```
    Do you want to integrate with an ITCAM Agent for WebSphere Applications?
     [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    You must install and configure ITCAM Agent for WebSphere Applications and its application support files to complete the installation and configuration of ITCAM Agent for WebSphere Applications. For more information about installing and configuring ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

    Important: When you configure data collection for ITCAM Agent for WebSphere Applications for applications servers in a profile where data collection is configured for application servers for ITCAM for SOA version 7.2, you must reconfigure and restart the Tivoli Enterprise Portal Server to capture ITCAM Agent for WebSphere Applications data in the topology views of ITCAM for SOA.

13. Enter 1 to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter 2 and skip to step 16 on page 278.

    You are prompted to enter the host name of ITCAM Agent for WebSphere Applications.

    ```
    Enter the host name or IP address of the ITCAM Agent for
    WebSphere Applications TEMA:
    [default is: 127.0.0.1]:
    ```

14. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. The monitoring agent is on the local host, so you do not have to change the default.

    You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

    ```
    Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
    [default is: 63335]:
    ```

    You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications monitoring agent. This communication is on the local host; the default port is 63335. You can change the port at a later time, but it is most convenient to set it when initially configuring the data collector.

15. Enter the port number of the monitoring agent.

The utility prompts you for the server alias. The alias is the name of the node in Tivoli Enterprise Portal that contains the monitoring information for this application server instance. The default is the node name combined with the server name.

```
Enter the server alias for server server1 in node node1  [default is: node1server1]:
```

Accept the default or enter another alias.

16. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM for Application Diagnostics Managing Server, installed on a separate Windows, Linux, or UNIX server, for deep-dive diagnostics. For information about installing the managing server, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    You are prompted to specify whether you want to integrate the data collector with a managing server.

    ```
    Do you want to integrate with an MS? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    Remember:

    - To integrate the data collector with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1.0.3 or later installed.
    - If you decide not to configure the managing server at this time, you can still configure the data collector to communicate with the managing server later.

17. Enter 1 to integrate with the managing server. Otherwise, enter 2 and skip to step 20.

    You are prompted to specify the host name of the managing server:

    ```
    Enter the host name  or IP address of the  MS
    [default is: 127.0.0.1]:
    ```

18. Enter the fully qualified host name of the managing server.

    You are prompted to specify the port number of the managing server:

    ```
    Enter the code base port number of the MS
    [default is: 9122]:
    ```

    The port number is codebase port on which the managing server is listening.

    Tip: The port number is specified in the key PORT_KERNEL_CODEBASE01 in the ITCAM61_MS_CONTEXT.properties file in the managing server home directory. For more information, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration tool attempts to connect to the managing server and retrieve the value for the managing server home directory. If successful, the tool displays a message similar to the following message:

    ```
    MS home directory is: C:\IBM\itcam\WebSphere\MS
    ```

19. If the connection to the managing server is *not* successful, you are prompted to enter the value of the managing server home directory:

    ```
    Enter ITCAM Managing Server install directory
    [default is C:\IBM\itcam\WebSphere\MS]:
    ```

    If prompted, enter the value of the managing server home directory.

20. The utility prompts you to specify whether you want to configure advanced settings for the managing server.

```
Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
[default is: 2]:
```

Enter 1 to configure advanced settings. Otherwise, enter 2 and skip to step 24.

21. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the managing server:

    ```
    Enter the RMI port numbers [default is: 8200-8299]:
    ```

    Tip: Make sure that the ports are not being blocked by a firewall or other applications.

    Enter the RMI port numbers.
22. You are prompted to enter the range of Controller RMI port numbers:

    ```
    Enter the range of Controller RMI port numbers
    [default is: 8300-8399]:
    ```

    Enter the RMI Controller port numbers.
23. You are prompted to enter the Remote File Sharing (RFS) port number of the managing server:

    ```
    Enter the RFS port number of the MS:  [default is: 9120]:
    ```

    The RFS server in the managing server kernel listens to the RFS port to accept incoming requests. Enter the RFS port number.
24. In the **Integration with ITCAM for Transactions** section, the utility provides an option for integrating the data collector with ITCAM for Transactions.

    Remember: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli Monitoring environment.
    You are prompted to specify whether you want to integrate with ITCAM for Transactions:

    ```
    Do you want to integrate with ITCAM for TT? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    After you configure the data collector to support ITCAM for Transactions, you must perform some additional configuration. For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.
25. Enter 1 to integrate the data collector with ITCAM for Transactions. Otherwise, enter 2 and skip to step 30.
26. You are prompted to specify the host name or IP address of the Transaction Collector, which is the component of ITCAM for Transactions that gathers metrics from multiple agents:

    ```
    Enter the host name or IP address for the Transaction Collector:
    [default is: 127.0.0.1]:
    ```
27. Enter the fully qualified host name or IP address of the Transaction Collector.
28. You are prompted to specify the port number that the data collector uses to connect to the Transaction Collector:

    ```
    Enter the port number for the Transaction Collector:
    [default is: 5455]:
    ```
29. Enter the port number for the interface to the Transaction Collector.
30. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

```
Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
[default is: 2]
```

ITCAM for WebSphere Application Server version 7.2 can be used to monitor the performance of the WebSphere Application Server. Performance monitoring infrastructure (PMI) metrics are gathered using ITCAM Data Collector for WebSphere and are displayed in the Tivoli Performance Viewer (TPV). The TPV is accessible from the WebSphere Application Server administrative console. ITCAM for WebSphere Application Server is installed separately from the WebSphere Application Server. For information about using ITCAM for WebSphere Application Server, see *IBM Tivoli Composite Application Manager for WebSphere Application Server version 7.2 Support for WebSphere Application Server version 8.5 Installation and User Guide*.

ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5 includes ITCAM Data Collector for WebSphere. Enter 1 to integrate ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter 2.

31. In the **Integration with Application Performance Diagnostics Lite** section, the utility provides an option for integrating the data collector with Application Performance Diagnostics Lite.

```
Do you want to integrate with Application Performance Diagnostics Lite
[1 - YES, 2 - NO]
[default is: 2]:
```

Application Performance Diagnostics Lite is a tool for diagnostic investigation of applications running on WebSphere Application Server and WebSphere Portal Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. For more information about installing and using Application Performance Diagnostics Lite, see the Application Performance Diagnostics Lite product documentation.

Enter 1 to integrate ITCAM Data Collector for WebSphere with the Application Performance Diagnostics Lite. Otherwise, enter 2.

32. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

```
Do you want to specify a Garbage Collection log path? [1 - YES, 2 - NO]
[default is: 2]:
```

Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step 34.

33. You are prompted to specify the garbage collection log path:

```
Enter the GC log path:
```

Enter a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name.cell_name.node_name.server_name`*`.gc.log` for every configured application server instance.

Important: In the garbage collection log path, you can use WebSphere variables such as `${SERVER_LOG_ROOT}`. However, do not use templates, such as `%pid`.

34. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that is to be applied to the specified application server instances:

```
 1) List of servers selected

   - WAS server: co098170Node01Cell.co098170Node01.server1(AppSrv01)
       WAS cell: co098170Node01Cell
        WAS node: co098170Node01

       WebSphere Profile home    :
          C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01

       wsadmin location          :
         C:\Program Files\IBM\WebSphere\AppServer\bin\wsadmin.bat

                     WAS version : 8.0.0.0
                      Deployment : Standalone
                        JVM mode : 32
              Configuration home : C\IBM\ITM\dchome\7.2.0.0.4

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

       TEMA hostname or IP address : 127.0.0.1
                TEMA port number : 63335
                      Monitor GC : No

 4) Integrate with ITCAM for AD Managing Server : No

       MS hostname or IP address : 127.0.0.1
         MS codebase port number : 9122
               MS home directory : C:\IBM\itcam\WebSphere\MS

 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with Application Performance Diagnostics Lite : No

 8) Advanced settings :

       Set Garbage Collection log path : No

You may accept or update your configuration choices for the following sections:
 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Integrate with Application Performance Diagnostics Lite
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'.
To accept you configuration without modifying, enter 'a'.
To quit the selection, enter 'q':
```

The example of the summary section is from a Windows platform. An example of a WebSphere Profile home on a Linux or UNIX platform is /opt/IBM/WebSphere/AppServer/profiles/AppSrv01. An example of a wsadmin location on a Linux or UNIX platform is /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh. An example of configuration home on a Linux or UNIX platform is /opt/IBM/ITM/dchome/7.2.0.0.4.

The summary section provides options to reconfigure parts of the data collector configuration before applying the changes and an option to exit the configuration utility without applying your changes. Enter the number that represents the section you want to edit. Enter an asterisk (*) to reconfigure all sections. Enter a to accept your changes. Enter q to exit the utility without configuring the data collector.

35. When you enter a to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```
36. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.
37. The utility applies the changes and presents a status message to indicate that the configuration of the data collector for the profile is complete:

    ```
    Successfully executed config for Cell: co098170Node01Cell
    Node: co098170Node01 Profile: AppSrv01.
    ```
38. After configuring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

Data collection is configured for the specified application server instances.

Unconfiguring ITCAM Data Collector for WebSphere

If you no longer want the data collector to monitor one or more application server instances, you can unconfigure the data collector for them.

The ITCAM Data Collector for WebSphere Unconfiguration utility is a menu driven command-line utility for unconfiguring ITCAM Data Collector for WebSphere.

To unconfigure the data collector, complete the following procedure:

1. From a command line, navigate to the *DC_home*\bin directory on Windows systems or the *DC_home*/bin directory on Linux or UNIX systems.
2. Set the location of the Java home directory before you run the script. For example:

   On Windows systems:

   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```

   On Linux or UNIX systems:

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```
3. Run the following command to start the ITCAM Data Collector for WebSphere Unconfiguration utility.

   On Windows systems:

   ```
   DC_home\bin\unconfig.bat
   ```

   On Linux or UNIX systems:

   ```
   DC_home/bin/unconfig.sh
   ```

   The utility searches for all server instances that are monitored by the ITCAM Data Collector for WebSphere.

   Remember:

   - Application server instances must be running during the unconfiguration procedure.

- For Network Deployment environment, the Node Agent and Deployment Manager must also be running.

The utility prompts you to select one or more application server instances from the list of configured servers:

```
Choose one or more servers to unconfigure for data collection:
Application Servers configured by the current version:
 1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
Enter a number or numbers separated by commas, or enter * to select all:
```

4. Enter the number that corresponds to the application server instance to unconfigure for data collection or enter an asterisk (*) to unconfigure data collection for all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: `1,2,3`.
5. The utility prompts you to specify whether you want to create a backup of your current WebSphere Application Server configuration:

   ```
   Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
   [default is: 2]:
   ```

   Enter 1 to create a backup of the current configuration. Otherwise, enter 2 and skip to step 8.
6. The utility prompts you to specify the directory in which to store the backup of the configuration. For example:

   On Windows systems:

   ```
   Enter backup directory  [default is: C:\IBM\ITM_DC\dchome\7.2.0.0.4\data]:
   ```

   On Linux or UNIX systems:

   ```
   Enter backup directory  [default is: /opt/IBM/ITM_DC/dchome/7.2.0.0.4/data]:
   ```

   Specify a directory in which to store the backup of the configuration or accept the default directory.
7. The utility displays the name of the WebSphere home directory and the WebSphere profile for which a backup is created. For example:

   On Windows systems:

   ```
   WebSphere Home:C:\Program Files (x86)\IBM\WebSphere\AppServer
   WebSphere Profile:AppSrv01
   ```

   On Linux or UNIX systems:

   ```
   WebSphere Home:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01
   WebSphere Profile:AppSrv01
   ```
8. The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile that you specified:

   ```
   WebSphere Global Security is enabled.
   ```

   If global security is not enabled, skip to step 11 on page 284.
9. The utility prompts you to specify whether to retrieve security settings from a client properties file:

   ```
   Do you want to retrieve security settings from a client properties file
   (soap.client.props or sas.client.props)?
   [1 - YES, 2 - NO] [default is: 2]:
   ```

   The data collector communicates with the WebSphere Administrative Services using the RMI or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for an SOAP connection.

Enter 1 to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 11. Otherwise, enter 2 to enter the user name and password.

```
Enter WebSphere admin user name:
Enter WebSphere admin user password:
```

10. If you selected the option to back up the current WebSphere configuration, the utility starts backing up the configuration. For example: On Windows systems:

    ```
    Backing up profile: AppSrv01 home: C:\Program Files
    (x86)\IBM\WebSphere\AppServer\bin ...  Backup file
    C:\IBM\ITM_DC\dchome\7.2.0.0.4\data\v525400e96601Cell01.
    v525400e96601Node01.AppSrv01.WebSphereConfig_20120716161102.zip
    is successfully created
    ```

    On Linux or UNIX systems:

    ```
    Backing up profile: AppSrv01 home: /opt/IBM/WebSphere/AppServer/bin ...
    Backup file /opt/IBM/ITM_DC/dchome/7.2.0.0.4/data/
    v525400e96601Cell01.v525400e96601Node01.AppSrv01.
    WebSphereConfig_20120716161102.zip is successfully created
    ```

11. The utility unconfigures the data collector for the specified application server instances. A status message is displayed to indicate that the data collector was successfully unconfigured. For example:

    ```
    Successfully executed Unconfiguring for Cell: v525400597750Node01Cell
    Node: v525 400597750Node01 Profile: AppSrv01
    ```

12. After unconfiguring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector unconfiguration takes effect when the application server instances are restarted.

Data collection is unconfigured for the specified application server instances.

Reconfiguring ITCAM Data Collector for WebSphere

If you configured the data collector to monitor one or more application server instances, you can reconfigure the data collector using the ITCAM Data Collector for WebSphere Reconfiguration utility.

You can change the data collector connection to the following products or components:

- ITCAM Agent for WebSphere monitoring agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for SOA monitoring agent
- ITCAM for Transactions
- Tivoli Performance Viewer, available from the WebSphere administrative console
- Application Performance Diagnostics Lite

You can also reconfigure garbage collection settings.

To reconfigure data collection for one or more monitored application server instances, complete the following procedure:

1. From the command line, navigate to the `*DC_home*\bin` directory on Windows systems or the `*DC_home*/bin` directory on Linux or UNIX systems.
2. Set the location of the Java home directory before you run the utility. For example:

on Windows systems:

```
set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
```

on Linux or UNIX systems:

```
export JAVA_HOME=/opt/IBM/AppServer80/java
```

3. Run the following command to start the ITCAM Data Collector for WebSphere Reconfiguration utility.

   On Windows systems:

   ```
   DC_home\bin\reconfig.bat
   ```

   On Linux or UNIX systems:

   ```
   DC_home/bin/reconfig.sh
   ```

   Tip: Running this utility has the same effect as running the `config.bat` script with the `-reconfig` argument on Windows systems or the `config.sh` script with the `-reconfig` argument on Linux or UNIX systems.

4. The utility starts and displays the IP addresses of all network cards found on the local computer system. The utility prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```

5. Enter the number that corresponds to the IP address to use.

   The utility searches for all application server instances for which the data collector is configured on this host, and prompts you to select one or more application server instances from the list:

   ```
   Choose one or more servers to configure for data collection:
   Application Servers configured by the current version:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:  1
   ```

   Remember:

   - For a stand-alone environment, application server instances must be running during the configuration.
   - For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
   - Ensure that the application server instances that you select are the actual servers that host the applications or services that you want to monitor.

6. Enter the number that corresponds to the application server instance to reconfigure for data collection or enter an asterisk (*) to reconfigure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: `1,2,3`.

7. In the **Integration with ITCAM for SOA Agent** section, the utility provides an option for integrating the data collector with the ITCAM for SOA agent.

   ```
   Do you want to integrate with an ITCAM for SOA Agent? [1 - YES, 2 - NO]
   [default is: 2]: 1
   ```

   You must install and configure the ITCAM for SOA agent and its application support files, and optionally configure topology support to complete the installation and configuration of the ITCAM for SOA Agent. For more information about installing and configuring the ITCAM for SOA agent, see *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

Enter 1 to integrate the data collector with the ITCAM for SOA Agent. Otherwise, enter 2.

8. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with the ITCAM Agent for WebSphere Applications.

   When configuring data collection for ITCAM Agent for WebSphere Applications, you can integrate the data collector with ITCAM Agent for WebSphere Applications monitoring agent, or with the ITCAM for Application Diagnostics Managing Server, or with both.

   ```
   Do you want to integrate with an ITCAM Agent for WebSphere Applications?
    [1 - YES, 2 - NO] [default is: 2]: 1
   ```

   You must install and configure ITCAM Agent for WebSphere Applications and its application support files to complete the installation and configuration of ITCAM Agent for WebSphere Applications. For more information about installing and configuring the ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

   Important: When you configure data collection for ITCAM Agent for WebSphere Applications for applications servers in a profile where data collection is configured for application servers for ITCAM for SOA version 7.2, you must reconfigure and restart the Tivoli Enterprise Portal Server to capture ITCAM Agent for WebSphere Applications data in the topology views of ITCAM for SOA.

9. Enter 1 to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter 2 and skip to step 12.

   You are prompted to enter the host name of the ITCAM Agent for WebSphere Applications monitoring agent.

   ```
   Enter the host name or IP address of the ITCAM Agent for WebSphere
   Applications TEMA: [default is: 127.0.0.1]: 127.0.0.1
   ```

10. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. The monitoring agent is on the local host, so the default is correct.

    You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

    ```
    Enter the port number of the ITCAM Agent for
    WebSphere Application TEMA:
    [default is: 63335]: 63335
    ```

    You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications monitoring agent. This communication is on the local host; the default port is 63335.

11. Enter the port number of the monitoring agent.

    The utility prompts you for the server alias. The alias is the name of the node in Tivoli Enterprise Portal that contains the monitoring information for this application server instance. The default is the node name combined with the server name.

    ```
    Enter the server alias for server server1 in node node1  [default is: node1server1]:
    ```

    Accept the default or enter another alias.

12. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM Application Diagnostics Managing Server, installed on a separate UNIX or Windows server, for deep-dive diagnostics. For information

about installing the managing server, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

You are prompted to specify whether you want to integrate the data collector with a managing server.

```
Do you want to integrate with an MS? [1 - YES, 2 - NO]
[default is: 2]: 1
```

Remember:

- To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1.0.3 or later installed.
- If you decide not to configure the managing server at this time, you can still configure the data collector to communicate with the managing server later.

13. Enter 1 to integrate with the managing server. Otherwise, enter 2 and skip to step 16.

    You are prompted to specify the host name of the managing server:

    ```
    Enter the host name  or IP address of the  MS
    [default is: 127.0.0.1]: 127.0.0.1
    ```

14. Enter the fully qualified host name of the managing server.

    You are prompted to specify the port number of the managing server:

    ```
    Enter the code base port number of the MS
    [default is: 9122]: 9122
    ```

    The port number is codebase port on which the managing server is listening.

    Tip: The port number is specified in the key `PORT_KERNEL_CODEBASE01` in the `ITCAM61_MS_CONTEXT.properties` file in the managing server home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration utility attempts to connect to the managing server and retrieve the value for the managing server home directory. If successful, the utility displays a message similar to the following message:

    ```
    MS home directory is: C:\IBM\itcam\WebSphere\MS
    ```

15. If the connection to the managing server is *not* successful, you are prompted to enter the value of the managing server home directory:

    ```
    Enter ITCAM Managing Server Install Directory
    [default is C:\IBM\itcam\WebSphere\MS]:
    ```

    If prompted, enter the value of the managing server home directory.

16. The utility prompts you to specify whether you want to configure advanced settings for the managing server.

    ```
    Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
    [default is: 2]: 1
    ```

    Enter 1 to configure advanced settings. Otherwise, enter 2 and skip to step 20 on page 288.

17. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the managing server:

    ```
    Enter the RMI port numbers
    [default is: 8200-8299] 8200-8299
    ```

    Tip: Make sure that the ports are not being blocked by a firewall or other applications.

Enter the RMI port numbers.

18. You are prompted to enter the range of Controller RMI port numbers:

    ```
    Enter the range of Controller RMI port numbers
    [default is: 8300-8399]: 8300-8399
    ```

    Enter the RMI Controller port numbers.

19. You are prompted to enter the Remote File Sharing (RFS) port number of the managing server:

    ```
    Enter the RFS port number of the MS:  [default is: 9120]:
    ```

    The RFS server in the managing server kernel listens to the RFS port to accept incoming requests. Enter the RFS port number.

20. In the **Integration with ITCAM for Transactions** section, the utility provides an option for integrating the data collector with ITCAM for Transactions.

    Remember: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli Monitoring environment.
    You are prompted to specify whether you want to integrate with ITCAM for Transactions:

    ```
    Do you want to integrate with ITCAM for TT? [1 - YES, 2 - NO]
    [default is: 2]: 1
    ```

    After you configure the data collector to support ITCAM for Transactions, you must perform some additional configuration. For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.

21. Enter 1 to integrate the data collector with ITCAM for Transactions. Otherwise, enter 2 and skip to step 26.

22. You are prompted to specify the host name or IP address of the Transaction Collector, which is the component of ITCAM for Transactions that gathers metrics from multiple agents:

    ```
    Enter the host name or IP address for the Transaction Collector:
    [default is: 127.0.0.1]: 127.0.0.1
    ```

23. Enter the fully qualified host name or IP address of the Transaction Collector.

24. You are prompted to specify the port number of the interface to the Transaction Collector:

    ```
    Enter the port number for the Transaction Collector:
    [default is: 5455]: 5455
    ```

25. Enter the port number for the interface to the Transaction Collector.

26. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

    ```
    Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
    [default is: 2]
    ```

    ITCAM for WebSphere Application Server version 7.2 can be used to monitor the performance of the WebSphere Application Server. Performance monitoring infrastructure (PMI) metrics are gathered using ITCAM Data Collector for WebSphere and are displayed in the Tivoli Performance Viewer (TPV). The TPV is accessible from the WebSphere Application Server administrative console. ITCAM for WebSphere Application Server is installed separately from the WebSphere Application Server. For information about using ITCAM for WebSphere Application Server, see *IBM Tivoli Composite*

Application Manager for WebSphere Application Server version 7.2 Support for WebSphere Application Server version 8.5 Installation and User Guide.

ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server version 8.5 includes ITCAM Data Collector for WebSphere. Enter 1 to integrate ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter 2 and skip to step 27.

27. In the **Integration with Application Performance Diagnostics Lite** section, the utility provides an option for integrating the data collector with Application Performance Diagnostics Lite.

    ```
    Do you want to integrate with Application Performance Diagnostics Lite
    [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    Application Performance Diagnostics Lite is a tool for diagnostic investigation of applications running on WebSphere Application Server and WebSphere Portal Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. For more information about installing and using Application Performance Diagnostics Lite, see the Application Performance Diagnostics Lite product documentation.

    Enter 1 to integrate ITCAM Data Collector for WebSphere with the Application Performance Diagnostics Lite. Otherwise, enter `2` and skip to step 28.

28. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

    ```
    Do you want to specify a Garbage Collection log path? [1 - YES, 2 - NO]
    [default is: 2]: 2
    ```

    Enter 1 to select a garbage collection log path. Otherwise, enter `2` and skip to step 30.

29. You are prompted to specify the garbage collection log path:

    ```
    Enter the GC log path:
    ```

    Enter a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name.cell_name.node_name.server_name`*`.gc.log` for every configured application server instance.

    Important: In the garbage collection log path, you can use WebSphere variables such as `${SERVER_LOG_ROOT}`. However, do not use templates, such as `%pid`.

30. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that is to be applied to the specified application server instances:

    ```
     1) List of servers selected

       - WAS server: co098170Node01Cell.co098170Node01.server1(AppSrv01)
           WAS cell: co098170Node01Cell
            WAS node: co098170Node01

           WebSphere Profile home    :
              C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01

           wsadmin location          :
             C:\Program Files\IBM\WebSphere\AppServer\bin\wsadmin.bat
    ```

```
                     WAS version : 8.0.0.0
                      Deployment : Standalone
                        JVM mode : 32
              Configuration home : C\IBM\ITM\dchome\7.2.0.0.4


 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

       TEMA hostname or IP address : 127.0.0.1
                  TEMA port number : 63335
                        Monitor GC : No

 4) Integrate with ITCAM for AD Managing Server : No

       MS hostname or IP address : 127.0.0.1
         MS codebase port number : 9122
               MS home directory : C:\IBM\itcam\WebSphere\MS

 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with Application Performance Diagnostics Lite : No

 8) Advanced settings :

       Set Garbage Collection log path : No

You may accept or update your configuration choices for the following sections:
 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Integrate with Application Performance Diagnostics Lite
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'.
To accept you configuration without modifying, enter 'a'.
To quit the selection, enter 'q':
```

The example of the summary section is from a Windows platform. An example of a WebSphere Profile home on a Linux or UNIX platform is `/opt/IBM/WebSphere/AppServer/profiles/AppSrv01`. An example of a wsadmin location on a Linux or UNIX platform is `/opt/IBM/WebSphere/AppServer/bin/wsadmin.sh`. An example of configuration home on a Linux or UNIX platform is `/opt/IBM/ITM/dchome/7.2.0.0.4`.

The summary section provides options to change parts of the data collector configuration before applying the changes and an option to exit the configuration tool without applying your changes. Enter the number that represents the section that you want to edit. Enter an asterisk (*) to reconfigure all sections. Enter `a` to accept your changes. Enter `q` to exit the utility.

31. When you enter `a` to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

```
Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
[default is: 2]:
```

32. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.
33. The utility applies the changes and presents a status message to indicate that the reconfiguration of the data collector for the profile is complete:

    ```
    Successfully executed Reconfiguring for Cell: v525400597750Node01Cell
    Node: v525
    400597750Node01 Profile: AppSrv01
    ```
34. After reconfiguring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

Data collection is reconfigured for the specified application server instances.

Migrating data collectors to ITCAM Data Collector for WebSphere

A previous version or an earlier maintenance level of ITCAM Data Collector for WebSphere can be migrated interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

You can migrate the data collector to use ITCAM Data Collector for WebSphere if your application server instances are monitored by any of the following products or components:

1. ITCAM for WebSphere version 6.1.0.4 or later
2. WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
3. ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
4. ITCAM for WebSphere Application Server version 7.2
5. ITCAM for SOA version 7.1.1
6. An earlier maintenance level of the ITCAM Data Collector for WebSphere version 7.2 and later

For the procedure for migrating the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector to ITCAM Data Collector for WebSphere, see “Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere” on page 294.

To upgrade the monitoring of server instances to ITCAM Data Collector for WebSphere or to update the maintenance level of the data collector, complete the following procedure:

1. Set the location of the Java home directory before you run the utility. For example:

   on Windows systems:

   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```

   on Linux or UNIX systems:

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```
2. Run the following command to start the migration utility.

   On Windows systems:

   ```
   DC_home\bin\migrate.bat
   ```

On Linux or UNIX systems:

```
DC_home/bin/migrate.sh
```

3. The utility displays the IP addresses of all network cards that are found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```

4. Enter the number that corresponds to the IP address to use.

   The utility prompts you to specify from the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere.

   ```
   List of ITCAM agents where the data collector can be upgraded from a previous version
   or maintenance level to ITCAM Data Collector for WebSphere:

   1. ITCAM for WebSphere 6.1.0.4 or later
   2. ITCAM WebSphere Agent 6.2.0.4 or later
   [ITCAM for Web Resources 6.2]
   3. ITCAM Agent for WebSphere Applications 7.1
   [ITCAM for Application Diagnostics 7.1]
   4. ITCAM for WebSphere Application Server 7.2
   5. ITCAM for SOA 7.1.1.x
   6. Maintenance level update for ITCAM Data Collector for WebSphere 7.2 and later
   [ITCAM Agent for WebSphere Applications 7.2 and later,
   ITCAM for SOA 7.2 and later, IBM Application Performance Diagnostics Lite]
   Enter the number [default is: 1]:
   ```

   Enter the number that represents the agent.

   Important: To update the maintenance level of ITCAM Data Collector for WebSphere, enter 6.

   For the procedure for migrating the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector to version 7.2, see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 294.

5. The utility prompts you to specify the home directory of the previous version of the data collector.

   ```
   Enter the home directory of the data collector to be upgraded:
   ```

6. Enter the home directory of the previous version of the data collector. For example, `C:\IBM\ITM\TMAITM6\wasdc\7.1.0.2` on Windows systems or `/opt/IBM/ITM/li6263/yn/wasdc/7.1.0.2` on Linux or UNIX systems.

   If you are migrating ITCAM for WebSphere Application Server version 7.2 or performing a maintenance level update, skip to step 9 on page 293.

7. If the data collector was integrated with the ITCAM Agent for WebSphere monitoring agent, you are prompted to reenter the host name and port of the monitoring agent. If more than one version of the monitoring agent is available, you can connect the data collector to the correct version.

   ```
   Enter the host name or IP address of the ITCAM Agent for
   WebSphere Applications TEMA:
   [default is: 127.0.0.1]:
   ```

8. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. It is on the local host, so the default is correct.

   You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

```
Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
[default is: 63335]:
```

Enter the port number of the monitoring agent.

9. The utility searches for the list of application server instances that are configured by the specified data collector installation.

   The utility prompts you to select one or more application server instances from the list. The instances might be under different profiles.

   ```
   Choose a Server or Servers to be migrate
    1. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server3
    2. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server5
    3. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server1
   Enter a number or numbers separated by a comma, enter '*' to select all
   servers listed, or enter 'q' to quit the selection.
   ```

   Tip: If several instances under one profile are monitored, you must select them all for migrating at the same time.

   Remember:

   - For a stand-alone environment, application server instances must be running during the configuration.
   - For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.

10. Enter the number that corresponds to the application server instance whose data collector is to be migrated or enter an asterisk (*) to migrate the data collector of all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represents the servers. For example: `1,2,3`.

11. The utility determines whether WebSphere Global Security was enabled for each of the profiles that are impacted by the migration task.

12. If WebSphere Global Security is enabled on one or more profiles, the utility prompts you to specify whether to retrieve security settings from a client properties file:

    ```
    Do you want to retrieve security settings from a client properties file
    (soap.client.props or sas.client.props)?
    [1 - YES, 2 - NO] [default is: 2]:
    ```

    The data collector communicates with the WebSphere Administrative Services using the RMI or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for an SOA connection.

    Enter *1* to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 13 on page 294. Otherwise, enter *2* to enter the user name and password.

    ```
    Enter WebSphere admin user name:
    Enter WebSphere admin user password:
    ```

    Important: It might take some time to log in to the WebSphere Application Server administrative console.
    The utility prompts you for the user name and password for each profile where WebSphere Global Security is enabled.

13. The utility migrates data collection for each selected application server instance and displays a status message that indicates whether the migration of each server completed successfully.
14. When the utility completes the migration of all application server instances configured by the previous version of the data collector, it displays the following message:

    ```
    Migration of the Data Collector has successfully completed with return code 0.
    ```
15. After migrating the data collector, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

Remember: For server instances that were upgraded, do not use the configuration utility for the old data collector version.

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and Application Performance Diagnostics Lite for the application server instances. For more information, see "Reconfiguring ITCAM Data Collector for WebSphere" on page 284.

Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere

If your application server instances are being monitored by ITCAM for SOA version 7.1.1 WebSphere Application Server data collector, you can upgrade the data collector to use ITCAM Data Collector for WebSphere.

The ITCAM Data Collector for WebSphere Migration utility is a menu driven command-line utility for migrating previous versions of ITCAM Data Collector for WebSphere.

For the procedure for migrating the following data collector components to ITCAM Data Collector for WebSphere, see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2
- An earlier maintenance level of the ITCAM Data Collector for WebSphere version 7.2 and later

To update the maintenance level of any products that have ITCAM Data Collector for WebSphere as a component, including ITCAM for SOA, follow the procedure in "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 291.

Important: If an older version of ITCAM Agent for WebSphere Applications is configured for application servers in the same profile as ITCAM for SOA version 7.1.1, migrate the data collector provided with ITCAM Agent for WebSphere Applications. Then, reconfigure the data collector to integrate it with the ITCAM for SOA monitoring agent. You must not run the migration utility to migrate the older version of the ITCAM for SOA WebSphere Application Server data collector.

To upgrade the monitoring of server instances from the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector to ITCAM Data Collector for WebSphere, complete the following procedure:

1. Set the location of the Java home directory before you run the utility. For example:

   on Windows systems:

   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```

   on Linux or UNIX systems:

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```

2. Run the following command to start the ITCAM Data Collector for WebSphere Migration utility.

   On Windows systems:

   ```
   DC_home\bin\migrate.bat
   ```

   On Linux or UNIX:

   ```
   DC_home/bin/migrate.sh
   ```

3. The utility displays the IP addresses of all network cards that are found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```

4. Enter the number that corresponds to the IP address to use.

   The utility prompts you to specify the type of agent that you want to migrate to ITCAM Data Collector for WebSphere.

   ```
   List of ITCAM agents where the data collector can be upgraded from a previous version
   or maintenance level to ITCAM Data Collector for WebSphere:

   1. ITCAM for WebSphere 6.1.0.4 or later
   2. ITCAM WebSphere Agent 6.2.0.4 or later
   [ITCAM for Web Resources 6.2]
   3. ITCAM Agent for WebSphere Applications 7.1
   [ITCAM for Application Diagnostics 7.1]
   4. ITCAM for WebSphere Application Server 7.2
   5. ITCAM for SOA 7.1.1.x
   6. Maintenance level update for ITCAM Data Collector for WebSphere 7.2 and later
   [ITCAM Agent for WebSphere Applications 7.2 and later,
   ITCAM for SOA 7.2 and later, IBM Application Performance Diagnostics Lite]
   Enter the number [default is: 1]:
   ```

   Enter 5 to migrate ITCAM for SOA version 7.1.1.

5. The utility prompts you to specify the WebSphere Application Server home directory where the previous version of the ITCAM for SOA version 7.1.1 data collector is configured.

   ```
   Specify SOA Websphere Home Directory:
   ```

6. The utility searches for all profiles under the specified home directory and prompts you to select a profile:

   ```
   List of WebSphere profiles discovered:
     1. AppSrv01
   Enter a number [default is: 1]:
   ```

7. Enter the number that corresponds to the WebSphere Application Server profile you want to configure.

   The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile that you specified:

   ```
   WebSphere Global Security is enabled.
   ```

If global security is not enabled, skip to step 9.

8. The utility prompts you to specify whether to retrieve security settings from a client properties file:

   ```
   Do you want to retrieve security settings from a client properties file
   (soap.client.props or sas.client.props)?
   [1 - YES, 2 - NO] [default is: 2]:
   ```

   The data collector communicates with the WebSphere Administrative Services using the RMI or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOAP connection.

   Enter `1` to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 9. Otherwise, enter `2` to enter the user name and password.

   ```
   Enter WebSphere admin user name:
   Enter WebSphere admin user password:
   ```

9. The utility searches for all application server instances under the specified profile. The utility displays all servers that are not configured yet for data collection and all servers that have been configured to use the same maintenance level of ITCAM Data Collector for WebSphere.

   The utility prompts you to select application server instances from the list:

   ```
   Choose one or more servers to configure for data collection:
   Application servers not yet configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:
   ```

   Important:

   - For a stand-alone environment, application server instances must be running during the configuration.
   - For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
   - Ensure that the application server instances that you select are the actual servers that host the BPM applications or services that you want to monitor.

10. Enter the number that corresponds to the application server instance to configure for data collection or enter an asterisk (*) to configure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represents the servers. For example: `1,2,3`.

    The utility displays a summary list. By default, it configures the migrated instances to integrate with ITCAM for SOA only. You can specify other configurations.

    ```
    +----------------------------------------------------------------------+
    |                                                                      |
    |  Data collector configuration summary                                |
    |                                                                      |
    +----------------------------------------------------------------------+

    Each of the servers will be configured for data collection

     1) List of servers selected
    ```

```
   - WAS server: IBM-6DA7F9C6EE6Node02Cell.IBM-6DA7F9CNode02.server1
(AppSrv02)
       WAS cell: IBM-6DA7F9C6EE6Node02Cell
        WAS node: IBM-6DA7F9C6EE6Node02

       WebSphere Profile home    :
         C:\Program Files\IBM\WebSphere\AppServer80\profiles\AppSrv02

       wsadmin location          :
         C:\Program Files\IBM\WebSphere\AppServer80\bin\wsadmin.bat

                     WAS version : 8.0.0.0
                      Deployment : Standalone
                        JVM mode : 32
              Configuration home : C\IBM\ITM\dchome\7.2.0.0.4

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : No

 4) Integrate with ITCAM for AD Managing Server : No

 5) Integrate with ITCAM for Transactions : No

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with Application Performance Diagnostics Lite : No

 8) Advanced settings :

       Set Garbage Collection log path : No

Configuration sections:

 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Integrate with Application Performance Diagnostics Lite
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'.
To accept your
configuration without modifying, enter 'a'. To quit the selection, enter 'q'.:
```

The example of the summary section is from a Windows platform. An example of a WebSphere Profile home on a Linux or UNIX platform is /opt/IBM/WebSphere/AppServer/profiles/AppSrv01. An example of a wsadmin location on a Linux or UNIX platform is /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh. An example of configuration home on a Linux or UNIX platform is /opt/IBM/ITM/dchome/7.2.0.0.4.

11. To enable integration with products and components other than ITCAM for SOA, select the corresponding number. For details on the configuration, see “Configuring ITCAM Data Collector for WebSphere” on page 274. Otherwise, to accept the configuration, enter a.

    You are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

12. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.

13. The utility applies the changes and presents a status message to indicate that the configuration of the data collector for the profile is complete:

    ```
    Successfully executed config for Cell: co098170Node01Cell
    Node: co098170Node01 Profile: AppSrv01.
    ```

14. After migrating the data collector, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and Application Performance Diagnostics Lite for the application server instances at the same time. For more information about reconfiguring application server instances, see "Reconfiguring ITCAM Data Collector for WebSphere" on page 284.

Configuring the data collector is silent mode

The ITCAM Data Collector for WebSphere configuration utilities support a *silent* mode. In this mode, no user interaction is required for configuration. Instead, the parameters are taken from a *response file*.

The following table provides a description of the configuration tasks that can be performed in silent mode by the utilities.

Table 41. Configuration tasks

Configuration task	Where to find the procedure
Configure the data collector to monitor application server instances within a WebSphere Application Server profile in silent mode.	"Configuring ITCAM Data Collector for WebSphere in silent mode"
Unconfigure the data collector in silent mode.	"Unconfiguring ITCAM Data Collector for WebSphere in silent mode" on page 305
Migrate an older version of the data collector to ITCAM Data Collector for WebSphere in silent mode or update the maintenance level of ITCAM Data Collector for WebSphere in silent mode.	"Migrating ITCAM Data Collector for WebSphere in silent mode" on page 308
Migrate the WebSphere Application Server data collector provided by ITCAM for SOA version 7.1.1 to ITCAM Data Collector for WebSphere in silent mode.	"Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode" on page 312

Important: When you create or edit a silent response file that contains unicode characters, make sure the file is saved using UTF-8 encoding. If you save the file using a different encoding scheme, for example ISO-8858, an error is displayed during the configuration task that indicates that the utility was unable to access the file.

Configuring ITCAM Data Collector for WebSphere in silent mode

ITCAM Data Collector for WebSphere can be configured interactively with the ITCAM Data Collector for WebSphere Configuration utility. If you want to configure many application server instances, it might be more convenient to configure the data collector in silent mode.

Important: In an ITCAM for Application Diagnostics deployment, do not configure the data collector to monitor an instance of WebSphere Application Server that hosts the Managing Server Visualization Engine (MSVE). However, you can use the data collector to monitor any other WebSphere Application Server instances that are on the same node.

When you configure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_config.txt`, is packaged with the configuration utility. The file is available in the `*DC_home*\bin` directory on Windows systems or the `*DC_home*/bin` directory on Linux and UNIX systems. The *DC_home* variable is the location where the data collector is installed.

A sample of a properties file is displayed in "Sample properties file" on page 302.

Complete the following steps to perform a silent configuration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*`\bin` directory on Windows systems or the *DC_home*`/bin` directory on Linux and UNIX systems.
3. Run the following command:

   Windows systems:

   ```
   config.bat -silent [dir_path]\silent file
   ```

   UNIX or Linux systems:

   ```
   config.sh -silent [dir_path]/silent file
   ```
4. After configuring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Properties file

When you create your properties file, keep in mind the following considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: *property* = *value*.

  property
  Name of property. The list of valid properties that you can configure is shown in Table 42 on page 300.

  value Value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case-sensitive.

Table 42 on page 300 describes the properties that are available when configuring the data collector in silent mode:

Table 42. Available properties for running the configuration utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
Integration of the data collector with the ITCAM for Application Diagnostics Managing Server	
ms.connect	Specifies whether the data collector is configured to connect to the managing server in an ITCAM for Application Diagnostics environment. Valid values are `True` and `False`.
ms.kernel.host	Specifies the fully qualified host name of the managing server.
ms.kernel.codebase.port	Specifies the codebase port on which the managing server is listening.
ms.am.home	Specifies the managing server home directory.
ms.am.socket.bindip	Specifies the IP address or host name to be used by the data collector to communicate with the managing server. If more than one network interface or IP address is configured on data collector computer system, choose one of them.
ms.firewall.enabled	Specifies whether a firewall is enabled on the data collector host or you have special requirements to change the RMI ports for the data collector. Valid values are *True* and *False*.
ms.probe.controller.rmi.port	If the data collector is behind a firewall or you have special requirements to change the Controller RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: `ms.probe.controller.rmi.port=8300-8399` or ms.probe.controller.rmi.port=8300.
ms.probe.rmi.port	If the data collector is behind a firewall, or you have special requirements to change the RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: `ms.probe.rmi.port=8200-8299` or `ms.probe.rmi.port=8200`.
Integration of the data collector with the ITCAM for Transactions	
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are `True` and `False`.
ttapi.host	Specifies the host name of the ITCAM for Transactions Transaction Collector to connect to.
ttapi.port	Specifies the port of the Transaction Collector to connect to.
Integration of the data collector with the ITCAM for SOA	
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration.
Integration of the data collector with the Tivoli Performance Monitoring	
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Monitoring when the data collector is included as part of ITCAM for WebSphere Application Server version 8.5. Tivoli Performance Monitoring is accessed with the WebSphere Application Server administrative console. Valid values are *True* and *False*.
Integration of the data collector with the Application Performance Diagnostics Lite	
de.enable	Specifies whether to integrate the data collector with the Application Performance Diagnostics Lite. Application Performance Diagnostics Lite is a tool for diagnostic investigation of applications that run on WebSphere Application Server and WebSphere Portal Server. Valid values are `True` and `False`.
Integration of the data collector with the ITCAM Agent for WebSphere Applications monitoring agent	

Table 42. Available properties for running the configuration utility in silent mode (continued)

Property	Comment
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. Valid values are `True` and `False`. Set this property to `False` if you plan to connect ITCAM Agent for WebSphere Applications with the managing server only or you do not have ITCAM Agent for WebSphere Applications installed and do not plan to install it.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM Agent for WebSphere Applications monitoring agent.
WebSphere Application Server backup	
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are `True` and `False`.
was.backup.configuration.dir	Specifies the location of the backup directory.
Advanced configuration settings	
was.gc.custom.path	Specifies whether to set a custom path for the Garbage Collection log.
was.gc.file	Specifies the path to the custom Garbage Collection log. Set this value to a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *profile_name.cell_name.node_name.server_name*`.gc.log` for every configured application server instance. **Important:** In the Garbage Collection log path, you can use WebSphere variables, such as `${SERVER_LOG_ROOT}`. However, do not use templates, such as %pid.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting. In a Network Deployment environment, specify the wsadmin connection to the Deployment Manger. In a stand-alone environment, specify the wsadmin connection to the server.
was.wsadmin.connection.type	Specifies the connection protocol for the wsadmin tool to use.
was.wsadmin.connection.port	Specifies the port that the wsadmin tool must use to connect to the WebSphere Application Server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log in to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
was.client.props	Specifies whether to retrieve security settings from a client properties file. Possible values are `True` and `False`.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile that you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	

Table 42. Available properties for running the configuration utility in silent mode (continued)

Property	Comment
was.appserver.server.name	Specifies the application server instance within the application server profile to configure. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

When you run the configuration utility in silent mode, the configuration parameters are read from a simple text properties file, *silent_file*, that you create in advance. A typical properties file on a Windows platform might look similar to the following example:

```
#############################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Configuration Utility (config.sh|bat) in <dc_home>/bin.
#Run config.sh|bat -silent [dir_path]/<properties_file> to configure the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#You can integrate the data collector with the following components:
#  ITCAM for Application Diagnostics Managing Server
#  ITCAM for Transactions
#  ITCAM for SOA agent
#  Tivoli Performance Viewer (for ITCAM for WebSphere Application Server)
#  ITCAM Diagnostics Tool
#  ITCAM Agent for WebSphere Applications monitoring agent
#
#Considerations:
#
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.

#Modify Garbage Collection log path:
#The full path to the GC log file must exist.
#The server name, cell name, and node name are appended to the GC log file name.
#
#Connect to WebSphere Administrative Services:
#The utility determines the connection type and port automatically.
#If the utility cannot determine the values, uncomment, and override the default values.
#
#Servers:
#You can configure multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
#############################################################################################

[DEFAULT SECTION]

#  IP addresses to use:
#default.hostip=9.9.9.9

#  ITCAM for Application Diagnostics Managing Server:
ms.connect=False
ms.kernel.host=msservername.yourcompany.com
ms.kernel.codebase.port=9122
ms.am.home=C:\IBM\itcam\WebSphere\MS
ms.am.socket.bindip=servername.yourcompany.com
#ms.firewall.enabled=
ms.probe.controller.rmi.port=8300-8399
ms.probe.rmi.port=8200-8299
```

```
#  ITCAM for Transactions:
ttapi.enable=False
ttapi.host=ttservername.yourcompany.com
ttapi.port=5455

#  ITCAM for SOA agent:
soa.enable=False

#  Tivoli Performance Viewer:
tpv.enable=True

#  ITCAM Diagnostics Tool:
de.enable=False

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=C:\IBM\ITM\dchome\7.2.0.0.4

#  Modify Garbage Collection log path:
#was.gc.custom.path=False
#was.gc.file=C:\test.log

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
#was.wsadmin.connection.type=SOAP
#was.wsadmin.connection.port=8881

#  WebSphere Global Security:
was.wsadmin.username=
was.wsadmin.password=
was.client.props=False

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

A typical properties file on a Linux or UNIX platform might look similar to the following example:

```
###########################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Configuration Utility (config.sh|bat) in <dc_home>/bin.
#Run config.sh|bat -silent [dir_path]/<properties_file> to configure the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#You can integrate the data collector with the following components:
#  ITCAM for Application Diagnostics Managing Server
#  ITCAM for Transactions
#  ITCAM for SOA agent
#  Tivoli Performance Viewer (for ITCAM for WebSphere Application Server)
#  ITCAM Diagnostics Tool
#  ITCAM Agent for WebSphere Applications monitoring agent
#
#Considerations:
#
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.

#Modify Garbage Collection log path:
#The full path to the GC log file must exist.
#The server name, cell name, and node name are appended to the GC log file name.
#
#Connect to WebSphere Administrative Services:
#The utility determines the connection type and port automatically.
#If the utility cannot determine the values, uncomment, and override the default values.
#
#Servers:
#You can configure multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
##########################################################################################

[DEFAULT SECTION]

#  IP addresses to use:
#default.hostip=9.9.9.9

#  ITCAM for Application Diagnostics Managing Server:
ms.connect=False
ms.kernel.host=msservername.yourcompany.com
ms.kernel.codebase.port=9122
ms.am.home=/opt/IBM/itcam/WebSphere/MS
ms.am.socket.bindip=servername.yourcompany.com
#ms.firewall.enabled=
ms.probe.controller.rmi.port=8300-8399
ms.probe.rmi.port=8200-8299

#  ITCAM for Transactions:
ttapi.enable=False
ttapi.host=ttservername.yourcompany.com
ttapi.port=5455

#  ITCAM for SOA agent:
soa.enable=False

#  Tivoli Performance Viewer:
tpv.enable=True

#  ITCAM Diagnostics Tool:
de.enable=False

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome/7.2.0.0.4

#  Modify Garbage Collection log path:
#was.gc.custom.path=False
#was.gc.file=/opt/test.log

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
#was.wsadmin.connection.type=SOAP
#was.wsadmin.connection.port=8881

#  WebSphere Global Security:
```

```
was.wsadmin.username=
was.wsadmin.password=
was.client.props=False

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=/opt/IBM/WebSphere/AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

Unconfiguring ITCAM Data Collector for WebSphere in silent mode

ITCAM Data Collector for WebSphere can be unconfigured interactively with the ITCAM Data Collector for WebSphere Unconfiguration utility. If you want to unconfigure many application server instances, it might be more convenient to unconfigure ITCAM Data Collector for WebSphere in silent mode.

When you unconfigure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_unconfig.txt`, is packaged with the unconfiguration utility. The file is available in the `*DC_home*\bin` directory on Windows systems or the `*DC_home*/bin` directory on Linux and UNIX systems. The *DC_home* variable is the location where the data collector is installed.

A sample of a properties file is presented in Table 43 on page 306.

Complete the following steps to perform a silent unconfiguration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*`\bin` directory on Windows systems or the *DC_home*`/bin` directory on Linux and UNIX systems.
3. Run the following command:

   Windows systems:

   `unconfig.bat -silent [dir_path]\silent file`

   UNIX or Linux systems:

   `unconfig.sh -silent [dir_path]/silent file`
4. After unconfiguring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: *property* = *value*.

property
This is the name of property. The list of valid properties that you can configure is shown in Table 43.

value This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. To use default values, you can comment out the property in the file.

- Passwords are in plain text.
- Properties and their values are case-sensitive.

Table 43 describes the properties that are available when unconfiguring the data collector in silent mode:

Table 43. Available properties for running the unconfiguration utility in silent mode

Property	Comment
WebSphere Application Server connecting settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to unconfigure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
Backup of the WebSphere Application Server configuration	
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server data collector configuration before unconfiguring the data collector. Valid values are `True` and `False`.
was.backup.configuration.dir	Specifies the location of the backup directory.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies an application server instance within the application server profile for which you want to unconfigure the data collector. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

When you run the unconfiguraiton utility in silent mode, the configuration parameters are read from a simple text properties file, *silent_file*, that you create in advance. A typical properties file on a Windows platform might look similar to the following example:

```
###################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Unconfiguration Utility (unconfig.sh|bat) in <dc_home>/bin.
#Run unconfig.sh|bat -silent [dir_path]/<properties_file> to unconfigure the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can configure multiple [SERVER] sections, one for each server to be configured within the profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
###################################################################################

[DEFAULT SECTION]

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
was.wsadmin.username=
was.wsadmin.password=

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=C:\Program Files\IBM\ITM\dchome\7.2.0.0.4\data

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

A typical properties file on a Linux or UNIX platform might look similar to the following example:

```
###########################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Unconfiguration Utility (unconfig.sh|bat) in
<dc_home>/bin.
#Run unconfig.sh|bat -silent [dir_path]/<properties_file> to unconfigure the data collector
silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can configure multiple [SERVER] sections, one for each server to be configured within
the profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
###########################################################################################

[DEFAULT SECTION]

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
was.wsadmin.username=
was.wsadmin.password=

#  WebSphere Application Server details:
```

```
was.appserver.profile.name=AppSrv02
was.appserver.home=/opt/IBM/WebSphere/AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome/7.2.0.0.4/data

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

Migrating ITCAM Data Collector for WebSphere in silent mode

A previous version or an earlier maintenance level of ITCAM Data Collector for WebSphere can be migrated interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

To migrate ITCAM for SOA WebSphere Application Server version 7.1.1 using the migration utility in silent mode, see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode" on page 312.

When you migrate the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate.txt`, is packaged with the migration utility. The file is available in the *DC_home*`\bin` directory on Windows systems or in the *DC_home*`/bin` directory on Linux and UNIX systems. The *DC_home* variable is the location where the data collector is installed. A sample of a properties file is presented in "Sample properties file" on page 310.

Complete the following steps to perform a silent migration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*`\bin` directory on Windows systems or the *DC_home*`/bin` directory on Linux and UNIX systems.
3. Run the following command:

   On Windows systems:

   ```
   migrate.bat -silent [dir_path]\silent file
   ```

   On Linux and UNIX systems:

   ```
   migrate.sh -silent [dir_path]/silent file
   ```

During a silent migration, you can also configure or reconfigure integration with: ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, ITCAM for WebSphere Application Server, and Application Performance Diagnostics Lite. Use the silent configuration parameters for these components, as described in "Configuring ITCAM Data Collector for WebSphere in silent mode" on page 298.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: *property* = *value*.

  property
  : This is the name of property. The list of valid properties that you can configure is shown in Table 44.

  value
  : This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case-sensitive.
- Available properties for running the migration utility in silent mode:

Table 44 describes the properties that are available when migrating the data collector in silent mode:

Table 44. Properties for the migration utility in silent mode

Property	**Comment**
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose data collector you want to migrate to ITCAM Data Collector for WebSphere. The value must be set to `AD`. **Important:** For all products, to update a maintenance level, set the `migrate.type` property to AD.
Location of data collector to be migrated	
itcam.migrate.home	Specifies the data collector home directory of the old version of the data collector. The directory is not deleted as part of the migration.
ITCAM Agent for WebSphere Applications monitoring agent settings	
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. Set this property to `False` if you do not want to connect the ITCAM Agent for WebSphere Applications with the monitoring agent, if you plan to connect the ITCAM Agent for WebSphere Applications with the managing server only, or if you do not have the ITCAM Agent for WebSphere Applications installed. Valid values are `True` and `False`. **Remember:** The managing server is not a component of ITCAM for Applications.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM for Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM for Agent for WebSphere Applications monitoring agent.
WebSphere Application Server connection settings	

Table 44. Properties for the migration utility in silent mode (continued)

Property	Comment
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting. In a Network Deployment environment, specify the wsadmin connection to the Deployment Manger. In a stand-alone environment, specify the wsadmin connection to the server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to migrate to the new version of the data collector. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

When you run the migration utility in silent mode, the configuration parameters are read from a simple text properties file, `silent_file`, that you create in advance. A typical properties file on a Windows platform might look similar to the following example:

```
#########################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Migration Utility (migrate.sh|bat)
in <dc_home>/bin.
#Run migrate.sh|bat -silent [dir_path]/<properties_file> to migrate an older
version of the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#Use this sample file to migrate the data collector of any of the following products:
#  ITCAM for WebSphere 6.1 (fix pack 4 or later)
#  WebSphere Data Collector 6.1 (fix pack 4 or later)
#  ITCAM Agent for WebSphere Applications 7.1
#  ITCAM for WebSphere Application Server 7.2
#
#Considerations:
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.
#
#Migration type:
#Important: Do not modify this value.
#
```

```
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
#
###########################################################################################

[DEFAULT SECTION]

#  IP address to use:
#default.hostip=9.9.9.9

#Migration type:
migrate.type=AD

#  Old data collector home directory:
itcam.migrate.home=c:\ibm\itm\tmaitm6\wasdc\71

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

#  Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=127.0.0.1
was.wsadmin.username=username
was.wsadmin.password=password

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourCellName
was.appserver.node.name=yourNodeName

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

A typical properties file on a Linux or UNIX platform might look similar to the following example:

```
###########################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Migration Utility (migrate.sh|bat) in
<dc_home>/bin.
#Run migrate.sh|bat -silent [dir_path]/<properties_file> to migrate an older version of the
data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#Use this sample file to migrate the data collector of any of the following products:
#  ITCAM for WebSphere 6.1 (fix pack 4 or later)
#  WebSphere Data Collector 6.1 (fix pack 4 or later)
#  ITCAM Agent for WebSphere Applications 7.1
#  ITCAM for WebSphere Application Server 7.2
#
#Considerations:
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.
#
#Migration type:
#Important: Do not modify this value.
#
```

```
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
#
############################################################################################

[DEFAULT SECTION]

#  IP address to use:
#default.hostip=9.9.9.9

#Migration type:
migrate.type=AD

#  Old data collector home directory:
itcam.migrate.home=/opt/IBM/ITM/tmaitm6/wsdc/71

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

#  Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=127.0.0.1
was.wsadmin.username=username
was.wsadmin.password=password

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
was.appserver.home=/opt/IBM/WebSphere/AppServer
was.appserver.cell.name=yourCellName
was.appserver.node.name=yourNodeName

#Note: As of now, was.appserver.server.name is the only supported parameter in this section
[SERVER]
was.appserver.server.name=server1


#Note: As of now, was.appserver.server.name is the only supported parameter in this section
##[SERVER]
#was.appserver.server.name=server2
```

Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode

The ITCAM for SOA version 7.1.1 WebSphere Application Server data collector can be migrated to ITCAM Data Collector for WebSphere interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

For the procedure for migrating the following data collector components to the ITCAM Data Collector for WebSphere, see "Migrating ITCAM Data Collector for WebSphere in silent mode" on page 308:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2

The procedure in “Migrating ITCAM Data Collector for WebSphere in silent mode” on page 308 can also be followed to update the maintenance level of any products that have ITCAM Data Collector for WebSphere as a component, including ITCAM for SOA.

Important: If an older version of ITCAM Agent for WebSphere Applications is configured for application servers in the same profile as ITCAM for SOA version 7.1.1, migrate the data collector provided with ITCAM Agent for WebSphere Applications. Then, reconfigure the data collector to integrate it with the ITCAM for SOA monitoring agent. You must not run the migration utility to migrate the older version of the ITCAM for SOA WebSphere Application Server data collector.

When you migrate the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate_soa.txt`, is packaged with the migration utility. The file is available in the *`DC_home`*`\bin` directory on Windows systems or in the *`DC_home`*`/bin` directory on Linux and UNIX systems. The *DC_home* variable is the location where the data collector is installed. A sample of a properties file is presented in “Sample properties file” on page 315.

Complete the following steps to perform a silent migration:

1. Specify configuration options in the properties file.
2. Go to the *`DC_home`*`\bin` directory on Windows systems or the *`DC_home`*`/bin` directory on Linux and UNIX systems.
3. Run the following command:

   On Windows systems:

   ```
   migrate.bat -silent [dir_path]\silent file
   ```

   On Linux and UNIX systems:

   ```
   migrate.sh -silent [dir_path]/silent file
   ```

While you are performing a silent migration, , you can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and Application Performance Diagnostics Lite for the application server instances at the same time. To do this, use the silent configuration parameters for these components, as described in “Migrating ITCAM Data Collector for WebSphere in silent mode” on page 308.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment. This means that you can use the number sign in passwords or for other uses.
- Each property is described on a separate line, in the following format: *property* = *value*.

  property
  : This is the name of property. The list of valid properties that you can configure is shown in: Table 45 on page 314.

  value
  : This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values

blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. To use default values, you can comment out the property in the file.

- Passwords are in plain text.
- Properties and their values are case-sensitive.

Table 45 describes the properties that are available when migrating the data collector in silent mode:

Table 45. Available properties for running the migration utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose agent you want to migrate to ITCAM Data Collector for WebSphere. The value must be set to `SOA`.
was.appserver.home	Location of the WebSphere Application Server home directory where the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector is configured. For example: `C:\Program Files\IBM\WebSphere\AppServer` on Windows systems and `/opt/IBM/WebSphere70/AppServer` on Linux and UNIX systems.
ms.connect	Specifies whether the data collector is configured to connect to the managing server in an ITCAM for Application Diagnostics environment. Valid values are `True` and `False`. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are `True` and `False`.
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration. Valid values are `True` and `False`.
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Viewer when the data collector is included as part of ITCAM for WebSphere Application Server 8.5. Tivoli Performance Viewer is accessed with the WebSphere Application Server administrative console. Valid values are `True` and `False`. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
de.enable	Specifies whether to integrate the data collector with the Application Performance Diagnostics Lite. Application Performance Diagnostics Lite is a tool for diagnostic investigation of applications that run on WebSphere Application Server and WebSphere Portal Server. Valid values are `True` and `False`. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.

Table 45. Available properties for running the migration utility in silent mode (continued)

Property	Comment
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. Valid values are `True` and `False`. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are `True` and `False`.
was.gc.custom.path	Specifies the path to the custom Garbage Collection log. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting. In a Network Deployment environment, specify the wsadmin connection to the Deployment Manger. In a stand-alone environment, specify the wsadmin connection to the server.
was.wsadmin.connection.type	Specifies the connection protocol for the wsadmin tool to use.
was.wsadmin.connection.port	Specifies the port that the wsadmin tool must use to connect to the WebSphere Application Server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to configure. **Important:** The silent response file can have multiple instances of this property.

Sample properties file

When you run the migration utility in silent mode, the configuration parameters are read from a simple text properties file, *silent_file*, that you create in advance. A typical properties file might look similar to the following example:

```
#########################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Migration Utility (migrate.sh|bat) in <dc_home>/bin.
```

```
#Run migrate.sh|bat -silent [dir_path]/<properties_file> to migrate an older version of
the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#Use this sample file to migrate the ITCAM for SOA 7.1.1 data collector.
#To migrate all other older versions of the data collector, use sample_silent_migrate.txt.
#
#Considerations:
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.
#
#Migration type:
# Important: Do not modify this value.
#
#Connect to WebSphere Administrative Services:
#The utility determines the connection type and port automatically.
#If the utility cannot determine the values, uncomment and override the default values.
#
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
###########################################################################################


[DEFAULT SECTION]
#IP address to use:
#default.hostip=9.9.9.9

#  Migration type:
migrate.type=SOA

#  Old WebSphere Application Server home directory:
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer80\AppServer

#  ITCAM for Application Diagnostics Managing Server:
ms.connect=False

#  ITCAM for Transactions:
ttapi.enable=False

#  ITCAM for SOA agent:
soa.enable=True

#  Tivoli Performance Viewer:
tpv.enable=False

#  ITCAM Diagnostics Tool:
de.enable=False

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=False

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False

#  Modify Garbage Collection log path:
was.gc.custom.path=False

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
was.wsadmin.username=
was.wsadmin.password=
#was.wsadmin.connection.type=SOAP
#was.wsadmin.connection.port=8881
```

```
#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

The example of the properties file is from a Windows platform. An example of a WebSphere Application Server home directory on a Linux or UNIX platform is `/opt/IBM/WebSphere80/AppServer`.

Limitations when monitoring SCA messages

Be aware of the following limitations on data collector support in the SCA environment:

- The data collector in the SCA environment supports monitoring, and not filtering. You can define monitoring controls to limit which SCA services or operations are monitored, but any filter controls defined to reject messages are ignored.
- Monitor control for the message content parameter (*none*, *headers*, *body*, *full*) only supports the *none* value. All other values are ignored and treated as *none*.
- The message length for SCA interactions is always reported as zero.
- The SCA data collector supports correlation of cross-module flows with SCA binding or Web service binding.
- The SCA data collector does not support remote host or remote IP address.

Removing duplicate WebSphere Application Server nodes

If you configure data collection for a WebSphere Application Server runtime environment, duplicates operations might display in the Interaction Details View of the Operation Flows workspace on the Tivoli Portal Server. After you upgrade from ITCAM for SOA version 7.1.1 fix pack 3, when metric files are loaded, a Websphere application server instance that was configured in ITCAM for SOA version 7.1.1 might be duplicated. The `kd4CleanupDuplicateNodes` utility that is provided with ITCAM for SOA version 7.2 Fix Pack 1 removes duplicate server instances from the SOA Domain Management Server database.

To remove duplicate server instances from the SOA Domain Management Server database, complete the following steps:

1. From a command-line window, navigate to the following directory:
   - On Windows systems, navigate to the *ITCAM4SOA_HOME*`\KD4\latest\bin` directory.
   - On Linux or UNIX systems, navigate to the *ITCAM4SOA_HOME*`/KD4/latest/bin` directory.
2. Run the `kd4CleanupDuplicateNodes` utility by following this syntax:

   ```
   kd4CleanupDuplicateNodes -dbuser username -dbpw password [-dbhost host]
    [-dbport port] [-dbtype type] [-dbname dbname]
   ```

   Where:

   -dbuser

   Specifies the SOA Domain Management Server database login name.

-dbpw Specifies the SOA Domain Management Server database password for user dbuser.

-dbhost
(Optional) Specifies the hostname of the computer system where the SOA Domain Management Server database is located. The default value is localhost.

-dbport
(Optional) Specifies the port number of the SOA Domain Management Server database. The default value is 50000.

-dbtype
(Optional) Specifies the database type. Valid values are DB2, MSSQL, or ORACLE. The default value is DB2.

-dbname
(Optional) Specifies the name of the SOA Domain Management Server database name. The default value is KD4SDMS.

Tip:

- On Window systems, run the command kd4CleanupDuplicateNodes.bat. On Linux and UNIX systems, run the command ./kd4CleanupDuplicateNodes.sh.
- If the database was not installed with default values, you must specify a value for options that are labelled optional.

3. The utility displays the list of application server instances that are configured in the SOA Domain Management Server. For example:

```
# ./kd4CleanupDuplicateNodes.sh -dbuser db2inst1 -dbpw db2inst1

  Host Name        Application Server Instance     Last Modification Date     DB Version
----------------------------------------------------------------------------------------
1 example.com:0    server1/wasNode01/wasNode01Cell  Mon Jan 07 12:56:02 CST 2013  7.1.1
2 example.com:2809 server1/wasNode01/wasNode01Cell  Tue Jan 08 09:37:25 CST 2013  7.2
3 example:2809     server1/wasNode02/wasNode02Cell  Tue Jan 08 09:37:25 CST 2013  7.2

Select a server instance to remove (type 0 to exit):
```

4. Locate a duplicate application server instance in the list.
5. Type the number of the duplicate server instance to delete and press Enter. For example:

```
# ./kd4CleanupDuplicateNodes.sh -dbuser db2inst1 -dbpw db2inst1

    Host Name      Application Server Instance     Last Modification Date    DB Version
---------------------------------------------------------------------------------------
1 example.com:0    server1/wasNode01/wasNode01Cell  Mon Jan 07 12:56:02 CST 2013  7.1.1
2 example.com:2809 server1/wasNode01/wasNode01Cell  Tue Jan 08 09:37:25 CST 2013  7.2
3 example:2809     server1/wasNode02/wasNode02Cell  Tue Jan 08 09:37:25 CST 2013  7.2

Select a server instance to remove (type 0 to exit): 1
```

To exit the utility without deleting a node, type 0.

6. The utility indicates the number of rows in the SOA Domain Management Server database that are removed. For example:

```
KD4DN0113I Selected Application Server Environment Key:
8b4c5fbc-bbb2-3112-a064-
7e55ba4fd04a
KD4DN0114I Set 7 rows to DELETED in sdms.relationship
```

```
KD4DN0114I Set 8 rows to DELETED in sdms.operinst
KD4DN0114I Set 1 row to DELETED in sdms.envnodemapping
KD4DN0114I Set 1 row to DELETED in sdms.appserverenv
KD4DN0115I Deletes have completed.
```

Duplicates server instances are removed from the Interaction Details View in the Tivoli Enterprise Portal.

Tip: In the SOA Domain Management Server database, the utility sets the DELETED column for each row to be removed. The rows are not removed until the cleanup routine runs on the database.

7. Repeat step 4 on page 318 to step 5 on page 318 for each duplicate node.
8. To exit the utility, type 0.

Logging and Filtering

The data collector in the SCA environment supports the monitor controls to define which SCA services and operations to monitor, but ignores the message content logging setting (*none*, *headers*, *body*, *full*) and never records message content.

The filter controls (rejection of messages) are not supported by the data collector in the SCA environment. This function is supported by IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server mediations to manage the rejection of messages. To record message content, use the log mediation function of IBM WebSphere Enterprise Service Bus or IBM WebSphere Process Server.

Configuring linking to the BPC Explorer

In the flyover and details window for an SCA human task or BPEL component node in the topology view in the Tivoli Enterprise Portal, a link to BPC Explorer can be available. To make it available, you must configure the BPC explorer root URL.

To customize the URL, use the command line on the Tivoli Enterprise Portal Server. Change to the `ITM_Home\CNPS\Products\KD4\bin` directory, and run the `kd4SDMSUrlConfig` utility.

This utility sets the URL for a specific monitored server instance. If you need to set the URL for several monitored server instances, you need to run it separately for each of the instances.

The syntax depends on whether the monitored instance is stand-alone or a part of a cluster.

To set the URL for a stand-alone instance:

```
kd4SDMSUrlConfig -mode bpcExplorer -sdmsHost localhost -sdmsPort port
  -sdmsUsername userName -sdmsPassword password -cellName cell
  -nodeName node -serverName server -url url
```

To set the URL for an instance that is a part of a cluster:

```
kd4SDMSUrlConfig -mode bpcExplorer -sdmsHost localhost -sdmsPort port
  -sdmsUsername userName -sdmsPassword password -cellName cell
  -clusterName cluster -url url
```

Where:

-mode Must be `bpcExplorer`.

-sdmsHost
The host name for the SDMS. As the command must be run on the Tivoli Enterprise Portal Server, and the SOA Domain Management Server is also running on the Tivoli Enterprise Portal Server, use `localhost`.

-sdmsUsername
The administrator user name for the SDMS.

-sdmsPassword
The administrator password for the SDMS.

-cellName
The name of the cell.

-clusterName
The name of the cluster.

-nodeName
The name of the node.

-serverName
The name of the server.

-url The root URL of the BPC explorer for this server instance, in the form `http[s]://`*`hostname`*`:`*`port/contextRoot`*. For example: `http://server.example.com/bpc`

Important: To delete the URL, instead of the `-url` option, use `-operation delete`. After you delete the URL, the link to the BPC Explorer is not available.

Chapter 8. Advanced configuration and customization of the ITCAM Data Collector for WebSphere

This section contains instructions for customizing your configuration of the ITCAM Data Collector for WebSphere.

Perform the procedures in each of the following sections, if they apply.

Properties files for the Data Collector

Several properties files control data collector configuration and behavior.

The properties files, and other files that are used by the data collector, are located under the *DC_home* directory.

For most common changes to this configuration, you must edit the toolkit properties file.

Important: After changing a configuration file, restart the monitored application server instance. Then the changes will take effect.

The toolkit properties file

The toolkit properties file is automatically created by the data collector at startup, using various input files. It is unique for every application server instance monitored by the data collector. Its name is *DC_home*/runtime/*appserver_version.node_name.server_name*/toolkit.properties.

Because this file is re-created at each data collector startup, **do not make any changes** to this file; if you do, they will be overwritten.

Instead, add the settings that you want to modify to the toolkit custom properties file. This file is named *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/toolkit_custom.properties. Settings in the toolkit custom properties file override the values in the toolkit properties file.

You can also set toolkit properties for all the application server instances that are monitored by this installation of the data collector. To do this, add the settings to the global toolkit custom properties file: *DC_home*/runtime/custom/toolkit_global_custom.properties. However, if a property is set in the instance-specific toolkit_custom.properties file, it overrides the value in the global file for this instance.

Important: If the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/toolkit_custom.properties or *DC_home*/runtime/custom/toolkit_custom.properties file does not exist, create it when you want to make changes. You might also have to create the custom directory.

Other properties files

The following properties files are unique for every application server instance monitored by the data collector:

- *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/cynlogging.properties defines the log file names and logging details for the Java portion of the data collector.
- *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/cyn-cclog.properties defines the log file names and logging details for the C++ portion of the data collector.

Important: You can integrate the data collector with ITCAM for Transactions using the configuration utilities. You can modify these settings using the toolkit_custom.properites file. For more information about configuring the transaction tracking API (TTAPI), see *IBM Tivoli Composite Application Agent for WebSphere Applications: Configuring and using TTAPI*.

Data collector log files

The default location for the log files generated by the data collector configuration utility is *DC_home*\data on Windows systems and *DC_home*/data on Linux and UNIX systems.

The following table describes log files generated before and during the configuration process

Table 46. Log files generated before and during the configuration process

Full path name	Description
DC_home/data/config-console.log	User input while the config or reconfig script is running.
DC_home/data/config-message.log	Messages generated while the config or reconfig script is running.
DC_home/data/config-trace.log	Debug messages generate while the config or reconfig script is running.
DC_home/data/reconfig.log	Log written during the reconfiguration of data collector for application servers.
DC_home/data/unconfig-console.log	User input while the unconfig script is running.
DC_home/data/unconfig-message.log	Messages generated while the unconfig script is running.
DC_home/data/unconfig-trace.log	Debug messages generated while the unconfig script is running.
DC_home/data/profile.cell.node.configdatacollector.log For example: default.beta85.tvt6080.configdatacollector.log	Log written by the wsadmin script (configDataCollector.py) during configuration updates to WebSphere Application Server.
DC_home/data/profile.cell.node.unconfigdatacollector.log For example: default.beta85.tvt6080.unconfigdatacollector.log	Log written by the wsadmin script (unconfigDataCollector.py) during unconfiguration updates to WebSphere Application Server.
DC_home/data/profile.findservers.log For example: default.findservers.log	Log generated by findSevers.py. The file is used for diagnosing problems with the find servers process.

Table 46. Log files generated before and during the configuration process (continued)

Full path name	Description
DC_home/data/node.server_valCheck.log For example: tvt6080_rd-test_valCheck.log	Log generated by WebSphere Application Sever validity checking.

The data collector trace files are stored by default in the following locations:

- On Windows systems: *DC_home*\logs\CYN\logs.
- On Linux and UNIX systems: *DC_home*/logs/CYN/logs.

Restriction: For log and trace file names that include *profile*, *cell*, *node*, or *server* variables, when any of these variables includes non-ascii characters, the non-ascii characters are converted to ascii characters.

WebSphere Global Security: setting the user name and password in client properties files

The data collector must communicate with WebSphere Administrative Services using the Remote Method Invocation (RMI) or the Simple Object Access Protocol (SOAP) protocol. If WebSphere Global Security is enabled, this communication requires a user name and password. You can set them when configuring the data collector to monitor an application server instance. For security reasons, you might prefer to encrypt the user name and password and store them in client properties files before configuring the data collector.

Use the sas.client.props file for an RMI connection, or the soap.client.props file for a SOAP connection.

Important: If you complete this operation, you must do it separately for each monitored application server profile.

Enabling user ID and password input from the sas.client.props file for RMI connector types

When you use an RMI connection to WebSphere Application Server and global security is enabled, you can use the ITCAM Data Collector for WebSphere configuration utilities to retrieve the user ID and password from a sas.client.props file.

To retrieve the user ID and password from the sas.client.props file, complete the following steps:

1. Set the following properties in the *AppServer_home*\profiles\profile_name\properties\sas.client.props file on Windows systems or in the *AppServer_home*/profiles/*profile_name*/properties/sas.client.props on Linux and UNIX systems:

   ```
   com.ibm.CORBA.loginSource=properties
   com.ibm.CORBA.securityEnabled=true
   com.ibm.CORBA.loginUserid=user_ID
   com.ibm.CORBA.loginPassword=password
   ```

2. Run the following command on Windows systems to encrypt the password:

   ```
   PropFilePasswordEncoder.bat path_to_props_file\sas.client.props
   com.ibm.CORBA.loginPassword
   ```

   Run it from the *AppServer_home*\profiles\profile_name\bin directory.

3. Run the following command on Linux and UNIX systems to encrypt the password:

   ```
   ./PropFilePasswordEncoder.sh path_to_props_file/sas.client.props
   com.ibm.CORBA.loginPassword
   ```

   Run it from the *AppServer_home*/profiles/*profile_name*/bin directory.

Enabling user ID and password input from the soap.client.props file for SOAP connector types

When you use a SOAP connection to WebSphere Application Server and global security is enabled, you can use the ITCAM Data Collector for WebSphere configuration utilities to retrieve the user ID and password from a soap.client.props file.

To retrieve the user ID and password from the soap.client.props file, complete the following steps:

1. Set the following properties in the *AppServer_home*\profiles*profile_name*\properties\soap.client.props on Windows systems and in the *AppServer_home*/profiles/*profile_name*/properties/soap.client.props file on Linux or UNIX systems:

   ```
   com.ibm.SOAP.securityEnabled=true
   com.ibm.SOAP.loginUserid=user_ID
   com.ibm.SOAP.loginPassword=password
   ```

2. Run the following command on Windows systems to encrypt the password:

   ```
   PropFilePasswordEncoder.bat
     AppServer_home\profiles\profile_name\properties\soap.client.props
     com.ibm.SOAP.loginPassword
   ```

   Run it from the *AppServer_home*\profiles*profile_name*\bin directory.

3. Run the following command on Linux or UNIX systems to encrypt the password:

   ```
   ./PropFilePasswordEncoder.sh
     AppServer_home/profiles/profile_name/properties/soap.client.props
     com.ibm.SOAP.loginPassword
   ```

   Run it from the *AppServer_home*/profiles/*profile_name*/bin directory.

Configuring the data collector when changing the application server version

If you upgrade the application server that is being monitored by the data collector from a 7.0 version to a 8.0 or 8.5 version, you must reconfigure the data collector to point to the updated instance of the application server.

Complete the following steps:

1. Unconfigure the data collector from all application server instances before the upgrade. In a Network Deployment environment, the Deployment Manager and the Node Agents must be running, but the application servers instances can be stopped.
2. Complete the upgrade of the application server.
3. For a non-Network Development environment, make sure that the application server instance is upgraded and started. For a Network Deployment environment, make sure that the Node Agent and Deployment Manager are upgraded and started; do not start the instances.

4. Use the ITCAM Data Collector for WebSphere Configuration utility to configure the data collector for each application server instance. For more information about configuring the data collector, see “Configuring ITCAM Data Collector for WebSphere” on page 274.
5. Start or restart the monitored application server instance. For information about restarting the application server, see “Restarting the application server” on page 351.

Configuring data collection for ITCAM for SOA when upgrading IBM BPM

Before you upgrade from IBM BPM version 7.5.1.1 or later to IBM BPM version 8.0 or later, you must unconfigure ITCAM Data Collector for WebSphere. After you upgrade to IBM BPM version 8.0 or later, reconfigure the data collector with the same settings.

Complete the following steps:

1. Unconfigure ITCAM Data Collector for WebSphere from all application server instances that you plan to migrate. Use the ITCAM Data Collector for WebSphere Unconfiguration utility to unconfigure the data collector.
2. Migrate from IBM BPM version 7.5.1.1 or later profile to IBM BPM version 8.0 or later profile.

   To maintain the historical data view for data that was collected for IBM BPM version 7.5.1.1 or later, migrate the application servers to a profile that has the same node name. In a Network Deployment environment, migrate the deployment manager and node profile.
3. Verify that the application server instances are migrated and started.

   In a Network Deployment environment, make sure that the Deployment Manager and Node Agent are migrated and started.

   Tip: If you migrated the WebSphere profile to a different host, install ITCAM for SOA version 7.2 on the target machine.
4. Reconfigure the data collector for all application server instances using the configuration utility. Specify the same parameters values that were used for IBM BPM version 7.5.1.1 or later.
5. Verify that the application servers are functioning correctly. Verify the connection from the data collector to the ITCAM for SOA monitoring agent and ITCAM for Transactions, as required.

Steps to complete if the IP address of the application server host is to be changed

If the IP address of the application server host is to be changed, complete the following procedure:

1. Use the ITCAM Data Collector for WebSphere Unconfiguration utility to unconfigure the data collector for this application server instance. For information about configuration, see “Unconfiguring ITCAM Data Collector for WebSphere” on page 282.
2. Stop the instance of the application server that is being monitored by the data collector. For information about stopping the application server, see “Stopping the application server” on page 354.
3. Complete the IP address change at the operating system and network level.

4. Start the instance of the application server that is being monitored by the data collector. For information about starting the application server, see “Starting the application server” on page 353.
5. Use the ITCAM Data Collector for WebSphere Configuration utility to configure the data collector again for this application server instance. For information about configuration, see “Configuring ITCAM Data Collector for WebSphere” on page 274.

What to do when deleting an application server profile

If you do not unconfigure the data collector before you delete an application server profile, data collector installation log and runtime data remains in the system, and running the WebSphere update command fails (typically with a `JACL failed` error message).

Unconfigure the data collector for all monitored application server instances in a profile before deleting it.

Using the root ID for the data collector installation when the application server is not owned and operated by the root ID

The installer can use whatever directories and files it requires. In addition, the installer can find most application server installations on the computer. But, if the application server is not owned and operated by root ID, you must complete the following tasks for the data collector to work correctly:

1. Use the chown command to change ownership of the data collector installation from root to the application server owner ID:
   ```
   chown -R wasOwnerId:wasGroupId DC_home
   ```
2. Make sure that the application server owner ID can write to the *DC_home*/`logs/CYN` directory:
   ```
   chown -R wasOwnerId:wasGroupId DC_home/logs/CYN
   ```

Increasing the heap size

To increase the heap size configuration, complete these steps from the WebSphere administrative console for each server that you want to configure for data collection:

1. Log in to the WebSphere Application Server administrative console.
2. Click **Server** > **Server Types** > **WebSphere Application Servers** and select the *server_name*.
3. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Additional Properties: Java Virtual Machine**.
4. Edit the **Maximum Heap Size** field. If the default is not specified then it defaults to `256`.

Setting a restrictive security policy for the data collector

By default, the data collector sets a permissive policy. This policy ensures that the data collector can run properly, and provides no other security protection. If you need a more restrictive policy, complete the following procedure to ensure that the policy becomes active and the data collector can still work properly.

The data collector sets the Java security policy file location for all monitored application server instances (`java.security.policy` system property) to *DC_home*`/itcamdc/etc/datacollector.policy`. You must edit this file in the following way:

1. Remove all existing content.
2. Copy the sample security policy for the data collector from the *DC_home*`/itcamdc/etc/datacollector.security.policy` file.
3. If ITCAM for Transactions is installed on the server, add a grant statement for the ITCAM for Transactions code base to the security policy file. Follow the model for the grant statements provided in the sample `datacollector.security.policy` file, but use the ITCAM for Transactions installation root directory in the codeBase statement.
4. Add your required security policy settings.
5. Save the file, and create a backup copy.

Important: Each time you configure or reconfigure the data collector for an application server instance, the file *DC_home*`/itcamdc/etc/datacollector.policy` might be overwritten. To ensure that your security policy remains active, restore this file from the backup copy after configuring or reconfiguring the data collector for any application server instance.

Manual changes to application server configuration for the data collector

You might want to configure and unconfigure data collector monitoring for an application server instance manually. Also, the data collector configuration might fail because of unexpected circumstances. You can restore the application server configuration manually if you created a backup of the configuration.

Important: You must make manual changes to the WebSphere Application Server configuration for data collectors as the WebSphere administrative user.

Restoring the application server configuration from a backup

If you configured a stand-alone application server instance for data collection either manually or with the configuration or migration utility and the application server fails to start, you must restore the application server configuration from a backup. If you did not create a backup, contact IBM Support.

In a Network Deployment environment, if you configured an application server instance for data collection manually or with the configuration or migration utility and the application server fails to start, you have the following options:

- You can restore the application server configuration from a backup configuration. If you did not create a backup, contact IBM Support.
- You can manually unconfigure the data collector. The Deployment Manager and the Node Agent on the application server must be running. For more information, see “Manually removing data collector configuration from an application server instance” on page 335.

This section applies only to the Windows, UNIX, and Linux platforms.

To apply the backup configuration using the **`restoreConfig`** command, complete one of the following procedures:

- In a non-Network Deployment environment:

1. Locate your backup configuration file. The default directory is *DC_home*/data. If several backup files are present, check the modification date and time of the file. It must be the date and time of the failed configuration. If you did not complete any other data collector configurations on the same host after the failed one, use the most recent file in the directory.
2. Stop all instances of the application server. Complete the steps in "Stopping the application server" on page 354.
3. Run the **restoreConfig** command from the *Appserver_home*/profiles/*profile_name*/bin directory. The syntax is:

Table 47. Syntax of the restoreConfig command in a non-Network Deployment environment

Operating system	Syntax	Example
Windows	restoreConfig.bat *full_path_to_backup_file*	restoreConfig.bat "*DC_home*\data\WebSphereConfig_2006-04-22.zip"
UNIX or **Linux**	./restoreConfig.sh *full_path_to_backup_file*	./restoreConfig.sh *DC_home*/data/WebSphereConfig_2006-04-22.zip

For more information about the arguments of the **restoreConfig** command, from the WebSphere Application Server v8.0 information center search for "restoreConfig command".

4. Start the instances of the application server. For more information about starting application server instances, see "Starting the application server" on page 353.

- In a Network Deployment environment:
  1. Locate your backup configuration file. The default directory is *DC_home*/data. If several backup files are present, check the modification date and time of the file; it must be the date and time of the failed configuration. If you did not complete any other data collector configurations on the same host after the failed one, use the most recent file in the directory.
  2. Stop all instances of application servers. Complete the steps in "Stopping the application server" on page 354.
  3. Create a temporary directory in any convenient path (*temp_directory*). On a UNIX or Linux host, create it under /tmp.
  4. Run the restoreConfig command from the *Appserver_home*/profiles/*profile_name*/bin directory. The syntax is:

Table 48. Syntax of restoreConfig command, Network Deployment environment

Operating system	Syntax	Example
Windows	restoreConfig.bat *full_path_to_backup_file*	restoreConfig.bat "C:\Program Files\IBM\itcam\WebSphere\DC\config_dc\backup\WebSphereConfig_2006-04-22.zip" -location *temp_directory*
UNIX or **Linux**	./restoreConfig.sh *full_path_to_backup_file*	./restoreConfig.sh /opt/IBM/itcam/WebSphere/DC/config_dc/backup/WebSphereConfig_2006-04-22.zip -location *temp_directory*

Running the restoreConfig command restores the original application server configuration to the temporary directory.

5. Copy the server.xml, variables.xml, and pmi-config.xml files from the following path:

```
temp_directory/restored_configuration_home/cells/cell_name/
nodes/node_name/servers/server_name
```

to the following path on the Deployment Manager host:

```
Appserver_home/profiles/profile_name/config/cells/cell_name/
nodes/node_name/servers/server_name
```

6. Complete a node sync from the Deployment Manager administrative console for the node.
7. In the Deployment Manager administrative console, save changes to the master configuration.
8. Start the instances of the application server. For more information, see "Starting the application server" on page 353.

Manually configuring the data collector to monitor an application server instance

You can configure the data collector to monitor an application server instance without using the configuration utility. You must create two settings files, and then manually add settings in the WebSphere Administrative Console. The runtime directory is created automatically when the data collector is started for the application server instance.

Important:

- You must make manual changes to the WebSphere Application Server configuration for data collectors as the WebSphere administrative user.
- You must be an experienced WebSphere administrator to make manual changes to the WebSphere Application Server for data collection. Any error in the manual configuration change can result in the application server not starting.
- If you manually configure the data collector to monitor application server instances, you cannot use the ITCAM Data Collector for WebSphere Unconfiguration utility to unconfigure the data collector.

Step 1. Create the `dcManualInput.txt` file

The `dcManualInput.txt` file contains some of the values needed for initial configuration of the data collector.

To create the `dcManualInput.txt` file, complete the following steps:

1. On Windows systems, copy the contents of the file *DC_home*`\itcamdc\etc\was\dcInput_manual.properties` into *DC_home*`\runtime\`*profile_name*`.`*cell_name*`.`*node_name*`.`*server_name*`.DCManualInput.txt`.

   On Linux or UNIX systems, copy the contents of the file *DC_home*`/itcamdc/etc/was/dcInput_manual.properties` into *DC_home*`/runtime/`*profile_name*`.`*cell_name*`.`*node_name*`.`*server_name*`.DCManualInput.txt`.
2. Edit the contents of the file.

   You must set the parameters in section 1 of the file according to the descriptions provided in Table 49. Do not change the parameters in section 2.

Table 49. Configuration Parameters for Section 1

Parameter	**Value**
local.hostname	The IP address or fully qualified domain name of the local system.

Table 49. Configuration Parameters for Section 1 (continued)

Parameter	Value
was.version	A short version number. Valid values are 70, 80, and 85. Use 70 for WebSphere Application Server 7.0 and all products based on it, 80 for WebSphere Application Server version 8.0 and all products based on it, and 85 for WebSphere Application Server version 8.5 and all products based on it.
itcam.home	ITCAM home directory.
was.nodename	Node name.
was.servername	Server name.
was.profilename	WebSphere profile name.
am.camtoolkit.gpe.dc.operation.mode	Operation mode of the data collector. Valid values are any combination of WR, MS, TT, SOA, ECAM, and DE, where: **WR** Integrates the data collector with the ITCAM Agent for WebSphere Applications monitoring agent. **MS** Integrates the data collector with the ITCAM for Application Diagnostics Managing Server. **TT** Integrates the data collector with ITCAM for Transactions. **SOA** Integrates the data collector with ITCAM for SOA monitoring agent. **ECAM** Integrates ITCAM for WebSphere Application Server data collector with Tivoli Performance Viewer (TPV). **DE** Integrates the data collector with Application Performance Diagnostics Lite. You must specify only the operation modes required. For example, if you are connecting the data collector to the ITCAM Agent for WebSphere Applications monitoring agent only, specify WR. Separate multiple operation modes with a comma.
interp	Platform code. For a complete list of platform codes, see Appendix D of the *IBM Tivoli Monitoring: Installation and Setup Guide*.
kwj.serveralias	(Optional) WebSphere Application Server alias name.
temagclog.path	(Optional) Garbage Collection log file path name. Enter a unique file name with full path. The path name must not include spaces.
tema.host	Host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. Mandatory if the operation mode includes ITCAM Agent for WebSphere Applications (WR).

Table 49. Configuration Parameters for Section 1 (continued)

Parameter	Value
tema.port	Port to use for communicating with the ITCAM Agent for WebSphere Applications monitoring agent. Mandatory if the operation mode includes ITCAM Agent for WebSphere Applications (WR).
ms.hostname	Host name or IP address of the ITCAM for Application Diagnostics Managing Server. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
kernel.codebase.port	Codebase port number of the Managing Server. The default is 9122. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
kernel.rfs.port	Managing Server kernel port number. The default is 9120. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
probe.controller.rmi.port	Range of Controller RMI port numbers. The default is 8300 - 8399. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
probe.rmi.port	Range of RMI port numbers. The default is 8200 is 8299. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
ms.home	Managing Server home directory. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
tt.connection.string	Host name or IP address and the port number of the Transaction Collector component of ITCAM for Transactions in the format of `tcp:`*`host_name`*`(IP):`*`port`*. Mandatory if the operation mode includes ITCAM for Transactions (TT).

Step 2. Create the `itcam_wsBundleMetaData.xml` file

The file `itcam_wsBundleMetaData.xml` contains some of the values needed for initial configuration of the data collector.

To create this file, complete the following steps:

1. Create a directory `wsBundleMetaData` under the *`DC_home`*`\runtime` directory on Windows system or under the *`DC_home`*`/runtime` directory on Linux or UNIX systems.
2. On Windows systems, copy the contents of the file *`DC_home`*`\itcamdc\etc\was\itcam_wsBundleMetaData_template.xml` into `itcam_wsBundleMetaData.xml`.

   On Linux and UNIX systems, copy the contents of the file *`DC_home`*`/itcamdc/etc/was/itcam_wsBundleMetaData_template.xml` into `itcam_wsBundleMetaData.xml`.
3. In the `itcam_wsBundleMetaData.xml` file, replace the variable `@{CONFIGHOME}` with the full path to your data collector home directory.

4. On Windows systems, place the file `itcam_wsBundleMetaData.xml` in the directory *DC_home*`\runtime\wsBundleMetaData`.

   On Linux and UNIX systems, place the file `itcam_wsBundleMetaData.xml` in the directory *DC_home*`/runtime/wsBundleMetaData`.

Step 3. Add settings with the WebSphere Administrative Console

Tip: The application server instance you are configuring for data collection must be running.

Complete the following steps:

1. Log in to the WebSphere administrative console.
2. Click **Servers**.
3. Expand **Server Type** and select **WebSphere application servers**.
4. Click the name of the server.
5. Expand **Java and Process Management** and select **Process Definition**.
6. Under the **Additional Properties** section, click **Java Virtual Machine**.
7. In the **Generic JVM arguments** field, add the following entries.

   ```
   -agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:$
   {ITCAMDCHOME}/toolkit/
   lib/bcm-bootstrap.jar -Djava.security.policy=
   ${ITCAMDCHOME}/itcamdc/etc/datacollector.policy -verbosegc -
   Dcom.ibm.tivoli.itcam.ai.runtimebuilder.
   inputs=${ITCAMDCHOME}/runtime/$name_of_the_file_created_DCManualInput.txt
   -Dsun.rmi.dgc.client.gcInterval=3600000
   -Dsun.rmi.dgc.server.gcInterval=3600000 -
   Dsun.rmi.transport.connectionTimeout=300000
   -Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData -
   Dam.wascell=$replace_with_was_cell_name
   -Dam.wasprofile=$replace_with_was_profile_name -
   Dam.wasnode=$replace_with_was_node_name
   -Dam.wasserver=$replace_with_was_server_name
   ```

   When adding the entries, take note of the following:

   - All entries must be on a single line.
   - Separate different arguments by spaces before the **-** sign, do not use spaces anywhere else.
   - Replace the following variables with the actual names:
     - *$name_of_the_file_created_DCManualInput.txt*
     - *$replace_with_was_cell_name*
     - *$replace_with_was_profile_name*
     - *$replace_with_was_node_name*
     - *$replace_with_was_server_name*
8. Click **Apply**.
9. In the Messages dialog box, click **Save**.
10. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
11. Click **Server** > **Application Servers** and select the *server_name*.
12. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Environment Entries**.

13. Depending on the operating system, the hardware platform, and the application server JVM, set the following environment entry:

Table 50. Environment Entry

Platform	Environment Entry name	Environment Entry value
AIX R6.1 (32 bit JVM)	`LIBPATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/aix533:${`*`ITCAMDCHOME`*`}/toolkit/lib/aix533/ttapi`
AIX R6.1 (64 bit JVM)	`LIBPATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/aix536:${`*`ITCAMDCHOME`*`}/toolkit/lib/aix536/ttapi`
AIX R7.1 (32 bit JVM)	`LIBPATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/aix533:${`*`ITCAMDCHOME`*`}/toolkit/lib/aix533/ttapi`
AIX R7.1 (64 bit JVM)	`LIBPATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/aix536:${`*`ITCAMDCHOME`*`}/toolkit/lib/aix536/ttapi`
HP-UX R11 (32 bit JVM)	`SHLIB_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/hp11:${`*`ITCAMDCHOME`*`}/toolkit/lib/hp11/ttapi`
HP-UX R11 (64 bit JVM)	`SHLIB_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/hp116:${`*`ITCAMDCHOME`*`}/toolkit/lib/hp116/ttapi`
HP-UX R11 Integrity (64 bit JVM)	`SHLIB_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/hpi116:${`*`ITCAMDCHOME`*`}/toolkit/lib/hpi116/ttapi`
Linux x86_64 R2.6 (64 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/lx8266:${`*`ITCAMDCHOME`*`}/toolkit/lib/lx8266/ttapi`
Linux Intel R2.6 (32 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/lx6263:${`*`ITCAMDCHOME`*`}/toolkit/lib/lx6263/ttapi`
Linux ppc R2.6 (32 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/lpp263:${`*`ITCAMDCHOME`*`}/toolkit/lib/lpp263/ttapi`
Linux ppc R2.6 (64 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/lpp266:${`*`ITCAMDCHOME`*`}/toolkit/lib/lpp266/ttapi`
Linux S390 R2.6 (32 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/ls3263:${`*`ITCAMDCHOME`*`}/toolkit/lib/ls3263/ttapi`

Table 50. Environment Entry (continued)

Platform	Environment Entry name	Environment Entry value
Linux S390 R2.6 (64 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/ls3266:${`*`ITCAMDCHOME`*`}/toolkit/lib/ls3266/ttapi`
Solaris R10 (32 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/sol293:${`*`ITCAMDCHOME`*`}/toolkit/lib/sol293/ttapi`
Solaris R10 (64 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/sol296:${`*`ITCAMDCHOME`*`}/toolkit/lib/sol296/ttapi`
Solaris R10 Opteron (64 bit JVM)	`LD_LIBRARY_PATH`	`/lib:${`*`ITCAMDCHOME`*`}/toolkit/lib/sol606:${`*`ITCAMDCHOME`*`}/toolkit/lib/sol606/ttapi`
Windows (32 bit JVM)	`PATH`	`/lib;${`*`ITCAMDCHOME`*`}/toolkit/lib/win32;${`*`ITCAMDCHOME`*`}/toolkit/lib/win32/ttapi`
Windows (64 bit JVM)	`PATH`	`/lib;${`*`ITCAMDCHOME`*`}/toolkit/lib/win64;${`*`ITCAMDCHOME`*`}/toolkit/lib/win64/ttapi`

14. Set the environment entry name `NLSPATH` to the following value: `${ITCAMDCHOME}/toolkit/msg/%L/%N.cat`
15. Click **Apply** and click **Save**.
16. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
17. Click **Server > Application Servers** and select the *server_name*.
18. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Java Virtual Machine** > **Additional Properties: Custom Properties**.
19. For the following name and value pairs, click **New**, enter the name and value, and click **Apply**:
    - Create an `am.home` property and set its value to the *`dchome`*`/itcamdc` directory path. For example:`am.home=/opt/IBM/ITM/dchome/7.2.0.0.4/itcamdc`
    - Create a `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild` property and set its value to true. For example: `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild=true`
    - Create a `ITCAM_DC_ENABLED` property and set its value to `true`, if the operation mode parameter in the `dcManualInput.txt` file includes `ECAM`.
    - Create a `TEMAGCCollector.gclog.path` property. If the generic Java Virtual Machine `verlogsegclog` argument is set, set the value of the `TEMAGCCollector.gclog.path` property to the same value. Otherwise, set the `TEMAGCCollector.gclog.path` property to `None`.

To identify the value of the `verlogsegclog` property, complete the steps:

a. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Java Virtual Machine**.

b. Locate the `verlogsegclog` property in the **Generic JVM arguments** field and note its value.

20. In the Messages dialog box, click **Save**.
21. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected. Click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
22. In the Navigation Pane, click **Environment** > **WebSphere Variables**.
23. Set the following variables. For each variable, choose the server name as the scope.
    - Set `ITCAMDCHOME` to `DC_home`.
    - Set `ITCAMDCVERSION` to the *version.release.maintenance_level* of the data collector. For example, `7.2.0.0.4`
24. Click **Apply** and click **Save**.
25. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
26. Restart the application server instance. The data collector reads the settings files and creates the runtime directory.

Manually removing data collector configuration from an application server instance

You can manually remove the data collector configuration from an application server instance, if any of the following conditions apply:

- In a non-Network Deployment environment, you manually added the data collector configuration to the application server instance and you want to unconfigure data collection. The application server instance must be running.
- In a Network Deployment environment, you manually added the data collector configuration to the application server instance and you want to unconfigure data collection. The Node Agent and Deployment Manager on the application server must be running.
- In a Network Deployment environment, you configured the application server instance for data collection manually and the application server fails to start. The Node Agent and Deployment Manager on the application server must be running.

If you configured a stand-alone application server instance for data collection either manually or with the configuration or migration utility and the application server fails to start, you must restore your WebSphere Application Server configuration with your backup configuration. For more information, see "Restoring the application server configuration from a backup" on page 327. If you did not create a backup, contact IBM Support.

Remember:

- You must make manual changes to the WebSphere Application Server configuration for data collectors as the WebSphere administrative user.

- Making manual changes to the WebSphere Application Server for data collection must be performed by an experienced WebSphere administrator only. Any error in the manual configuration change can result in the application server not starting.
- If you manually configure the data collector to monitor application server instances, you cannot use the ITCAM Data Collector for WebSphere Unconfiguration utility to unconfigure the data collector.

To manually remove the data collector configuration, complete the following procedure:

1. Log in to the WebSphere Administration Server Console.
2. Click **Servers**.
3. Expand **Server Type** and select **WebSphere application servers**.
4. Click the name of the server.
5. On the Configuration tab, under Server Infrastructure, expand **Java and Process Management** and select **Process Definition**.
6. Under the **Additional Properties** section, click **Java Virtual Machine**.
7. Under the **Additional Properties** section, click **Custom Properties**.
8. Remove any of the following JVM Custom Properties, if they are present:
   - `am.home`
   - `ITCAM.DC.ENABLED`
   - `TEMAGCCollector.gclog.path`
   - `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild`
   - `com.ibm.tivoli.jiti.injector.ProbeInjectorManagerChain.primaryInjectorFile` (if it is present)
9. Identify the JVM arguments added for ITCAM Data Collector for WebSphere:
   a. In the Navigation Pane, click **Environment** > **WebSphere Variables**.
   b. If you configured the application server for data collection manually, locate the JVM arguments you added manually.

      If you configured the application server for data collection with the configuration utilities, compare the value of the arguments `AM_OLD_ARGS` and `AM_CONFGI_JVM_ARGS` to determine which arguments were added by the configuration utility.
10. Click **Server** > **Application Server** and select the *server_name*.
11. On the Configuration tab, navigate to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Java Virtual Machine**.
12. In **Generic JVM Arguments**, remove the JVM arguments you identified in step 9 for ITCAM Data Collector for WebSphere.
13. Click **Apply** or **OK**.
14. In the **Messages** dialog box, click **Save**.
15. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
16. Remove environment entries added for ITCAM Data Collector for WebSphere.
    a. In the Configuration tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Environment Entries**.

b. Depending on the hardware platform, delete the LIBPATH (on AIX systems), SHLIB_PATH (on HP-UX systems), LD_LIBRARY_PATH (on Linux systems), or PATH (on Windows systems) environment entry.

c. Remove the NLSPATH environment entry.

17. Click **Apply** or **OK**.
18. In the **Messages** dialog box, click **Save**.
19. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
20. In the Navigation Pane, click **Environment** > **WebSphere Variables**.
21. Delete the following variables:
    - AM_CONFIG_JVM_ARGS
    - AM_OLD_JVM_ARGS
    - ITCAMDCHOME
    - ITCAMDCVERSION
22. In the **Messages** dialog box, click **Save**.
23. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
24. If you configured the server instance for data collection with the data collector configuration tool, rather than manually, complete the following steps:

    a. Navigate to the *DC_home*/runtime directory.

    b. Rename the file $profile.$cell.$node.$server.input.properties to $profile.$cell.$node.$server.input.properties.bak
25. If you are manually removing the data collector configuration from all application server instances in a profile, perform the following steps:

    a. Navigate to the $appserverhome/bin directory.

    b. Run the command osgiCfgInit.sh/bat -all on Windows systems or osgiCfgInit.sh -all on UNIX and Linux systems.
26. Restart the application server instance that was monitored by the data collector.

Customizing request information mapping

In some cases, you might have to change the information that identifies the requests monitored by the agent. This information includes the request name, and any data that can be displayed for the request (for example, the query text for an SQL request). To change the information, set up a custom request mapper configuration.

Define a custom request mapper configuration in an XML file. This file determines processing of the request data.

In this file, some built-in *symbols* represent values from the runtime context of the request. You can create additional symbols, which calculate new values. The calculation can include original request values, expressions, calls to Java methods (including methods in the monitored application), conditionals, and iteration over a set of values.

Then, you can *map* the contents of the symbols into the new request data that is provided to Tivoli Monitoring and ITCAM for Application Diagnostics Managing Server. If a particular variable in the request data is not mapped, the original value is retained.

Because different data is collected for request types, a custom request mapper configuration must be specific for a request type. You can configure different request mappers for different request types on the same data collector instance.

To set a custom request mapper configuration for a request type, you must make the following configuration changes:

- Enable custom request mapping for this type in the toolkit custom configuration file.
- Reference the XML file from the same configuration file.

XML file syntax

Create the XML file (for example, `request_custom.xml`). Place it in the *`DC_home`*`/runtime/custom` directory to use it for all application server instances, or in the *`DC_home`*`/runtime/`*`appserver_version.node_name.server_name`*`/custom` directory to use it for one application server instance. Ensure that it contains valid XML. The file must remain available while the configuration is in use.

Top level

The top-level tag is <gpe>. Within this tag, use the tag <runtimeConfiguration>. These tags have no attributes.

Within <runtimeConfiguration>, create a <requestMapperDefinition> tag. This tag must have a `type` attribute. Set it to the request mapper type name for the required request type; see Table 51 on page 348.

Within <requestMapperDefinition>, two tags must be present:

- <symbolDefinitions> contains all definitions of symbols. Symbols represent values that the agent calculates every time a request of this type is detected.
- <selection> contains the mapping of context keys to values. The keys represent the custom data that is passed to the agent. They are predefined for each request type (for more information about request mapper enabling properties and type names, see Table 51 on page 348). The mapping can be conditional.

Also, within the <runtimeConfiguration> tag, you can create a <requestMapperClassPath> tag. Within this tag, you can define JAR files. You can reference Java classes in these JAR files within Request Mapper definitions.

Defining an expression

To define symbols, you must use expressions. The agent evaluates the expressions to assign values to symbols.

Using data in an expression

An expression can use the following data:

- The input data symbols for the request type (for more information, see Table 51 on page 348).
- Other symbols described in the same request mapper definition.
- Numeric constants
- String constants (delimited with ", for example, "string")
- Boolean constants (true, TRUE, false, FALSE)
- The null constant.

If the value of a symbol is an instantiation of a Java class, expressions can contain references to fields and methods that are defined within the class. To refer to a field, use *symbol.fieldname*. To refer to a method, use *symbol.methodname*(*parameters*). The method call must return a value. For example, you can use the Java String methods with a symbol that has a String value.

To refer to a static field or method of a class, you can also use *classname.fieldname* and *classname.methodname*(*parameters*).

If a symbol refers to an array object, the expression can select an element (*symbol*[*selector*]) and determine the length of the array (*symbol*.length)

Operators

You can use the following operators in an expression:

- Boolean operators: AND, &, OR, |, NOT, !
- Comparison: ==, !=, GT, >, LT, <, GE, >=, LE, <=
- Numeric operators: +, -, *, /
- Parentheses to force order of evaluation: (,)

Important: You must escape the symbols <, >, and & in XML. Alternatively, you can use the GT (greater than), GE (greater than or equal), LT (less than), LE (less than or equal), and AND operators.

The expression can evaluate whether a value is an instance of a class, using the instanceof operator:

```
expression instanceof java.class.name
```

This operator, similar to the Java instanceof operator, produces a Boolean value. In this example, the value is true if the class to which the *expression* value belongs meets any of the following conditions:

- Is named *java.class.name*
- Is a direct or indirect subclass of the class identified by *java.class.name*.
- Implements, directly or indirectly, the interface identified by *java.class.name*.

The expression can also instantiate a new object of a Java class, using the new operator. This operator is similar to the Java new operator:

```
new java.class.name(expression1, expression2, ... expressionN)
```

Operator precedence

Operators are evaluated in order of precedence. Operators of the same order of precedence are evaluated from left to right. You can change the order of evaluation by using parentheses (and).

The order of precedence is:

1. `.` operator (method call or field reference)
2. `[ ]` (array element selector)
3. `new`
4. `!`, `NOT`
5. `*`, `/`
6. `+`, `-`
7. `GT`, `>`, `LT`, `<`, `GE`, `>=`, `LE`, `<=`, `instanceof`
8. `==`, `!=`
9. `AND`, `&`
10. `OR`, `|`

Example

```
$s1 >= ( 2 * ($s2.sampMethod($s3, true) + 1))
```

The agent evaluates this expression in the following way:

1. The `$s1` symbol is evaluated. It must yield a numeric value.
2. The `$s2` symbol is evaluated. It must yield a Java object.
3. The `$s3` symbol is evaluated.
4. The method `sampMethod` for the object resulting from the evaluation of `$s2` is called. The result of the evaluation of `$s3` is passed as the first parameter, and the Boolean value `true` is passed as the second parameter. The call to `sampMethod` must return a numeric value.
5. 1 is added to the result of step 4.
6. The result of step 5 is multiplied by 2.
7. The result of step 1 is compared with the result of step 6. If the result of step 1 is greater than or equal to the result of step 6, `true` is returned. Otherwise, `false` is returned.

Defining basic symbols

Within the <symbolDefinitions> tag, you can define a basic symbol using the <symbol> tag. For a basic symbol, define an expression that can be evaluated using other symbols.

Within the <symbol> tag, use the following tags:

`<name>`
The name of the symbol. It is a string and must start with the $ character.

`<eval>`
The expression that ITCAM must evaluate to produce the value for this symbol. For more information about defining expressions, see "Defining an expression" on page 338.

`<type>`
The type of the value that the symbol returns. Specify this value as a fully qualified Java class name, or a Java primitive. Specifying the type for the symbol is optional. If it is not defined, the Request Mapper attempts to establish the field type based on the expression. If the Request Mapper is unable to determine the symbol type before evaluating the expression, performance is affected. Therefore, for best performance, it is better to specify the type.

<args>
: The arguments for the symbol. This tag is optional; if it is specified, arguments must be supplied for evaluating the symbol. For more information, see "Defining symbol arguments."

Example

```
<symbol>
   <name>$doubles1</name>
   <eval>$s1*2</eval>
   <type>int</type>
</symbol>
```

This symbol returns double the value of another symbol, `$s1`.

Defining symbol arguments

Within the <args> tag of a symbol definition, you can define argument types for the symbol.

In this tag, use the <type> tag to specify the types of arguments. Specify this value as a fully qualified Java class name, or a Java primitive. You can specify any amount of <type> tags; each of these tags defines an argument.

In this case, the symbol must be referenced with arguments in parentheses:

```
$symbol(argument1,argument2...)
```

The number of arguments must be the same as the number of argument type definitions.

Within the symbol definition, refer to the first argument as `$p0`, the second argument as `$p1`, and so on.

A symbol with arguments works like a Java method. It takes input arguments, and returns a value that depends on the values of the arguments.

Example

```
<symbol>
   <name>$double</name>
   <eval>$p0*2</eval>
   <type>int</type>
   <args>
       <type>int</type>
   </args>
</symbol>
```

This symbol returns double the value of the argument. To evaluate it, supply a numeric argument: `$double(2)`, `$double($s1)`.

Defining iteration symbols

Within the <symbolDefinitions> tag, you can define an iteration symbol using the <iterationSymbol> tag. An iteration symbol represents a value that is acquired by iterating through a set of objects in a Java array, Enumeration, or Collection. For each of the members, Request Mapper evaluates one or more condition expressions. If an expression returns `true`, Request Mapper uses the member to calculate the return value. Once a member meets the condition expression, Request Mapper does not evaluate the rest of the members.

Within the <iterationSymbol> tag, use the following tags.

<name>
The name of the symbol. It is a string and must start with the `$` character.

<type>
The type of the value that the symbol returns. Specify this value as a fully qualified Java class name or a Java primitive. Specifying the type for the symbol is optional. If it is not defined, the Request Mapper attempts to establish the field type based on the expression. If the Request Mapper is unable to determine the symbol type before evaluating the expression, performance is affected. Therefore, for best performance, it is better to specify the type.

<args>
The arguments for the symbol. This tag is optional; if it is specified, arguments must be supplied for evaluating the symbol. For more information, see "Defining symbol arguments" on page 341.

<iterate over="*expression*">
Defines the object (array, Enumeration, or Collection) that contains the members to iterate through. The expression must return such an object. Request Mapper iterates over its members until either one of them causes a condition expression to return `true`, or no more members remain. Define the set of iteration expressions in tags within this tag:

> **<test>**
> Define the condition and return expression within this tag. An <iterate> tag can contain several <test> tags. In this case, Request Mapper evaluates all of them. If any condition expression is true, the symbol returns a value using the result expression in the same <test> tag, and no further evaluation is performed.
>
> > **<castTo>**
> > Optional: If this tag is present, specify the name of a Java type within it, as a fully qualified Java class name or a Java primitive. Request Mapper casts the iterated element to this type before evaluating the condition and return expressions. If this tag is not present, Request Mapper casts a member of an array to the array base type, and a member of an Enumeration or Collection to `java.lang.Object`. For an array member, the array base type is usually the correct choice; therefore, use this tag when iterating over an Enumeration or Collection.
> >
> > **<condition>**
> > An expression that must yield a Boolean value. Use `$iterElement` to refer to the element that is being iterated.
> >
> > **<return>**
> > If the expression in the <condition> tag returns `true`, Request Mapper evaluates the expression in the <return> tag. The iteration symbol returns the value that this expression produces. Use `$iterElement` to refer to the element that is being iterated.

<defaultValue>
Optional. If Request Mapper has iterated over all members of the object, but no condition expression has returned `true`, Request Mapper evaluates the expression in the <defaultValue> tag. The iteration symbol returns the value that the expression produces. If this tag is not present, the default value is `null`.

Examples

```
<iterationSymbol>
  <name>$userNameCookieValue</name>
  <iterate over="$httpServletRequest.getCookies()">
     <test>
        <condition>$iterElement.getName().equals("userName")</condition>
        <return>$iterElement.getValue()</return>
     </test>
   </iterate>
</iterationSymbol>
```

This symbol finds the cookie named "username", and returns its value. `$httpServletRequest.getCookies()` returns an array, so there is no need for the <castTo> element.

```
<iterationSymbol>
  <name>$headerNameStartingWithA</name>
  <iterate over="$httpServletRequest.getHeaderNames()">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.startsWith("A")</condition>
       <return>$iterElement</return>
    </test>
  </iterate>
</iterationSymbol>
```

This symbol finds the header with a name starting with "A", and returns its name. `$httpServletRequest.getHeaderNames()` returns an Enumeration, so the <castTo> element is required.

```
<iterationSymbol>
  <name>$determined_gender</name>
  <iterate over="$children">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("male")</condition>
       <return>"It's a boy"</return>
    </test>
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("female")</condition>
       <return>"It's a girl"</return>
    </test>
  </iterate>
  <defaultValue>"unknown"</defaultValue>
</iterationSymbol>
```

This symbol iterates over `$children`, which must be an array, Enumeration, or Collection of strings. If any of the strings equals "male", it returns "it's a boy". If any of the strings equals "female", it returns "it's a girl". Finally, if no string in the `$children` object equals either "male" or "female", the symbol returns "unknown".

Defining conditional symbols

Within the <symbolDefinitions> tag, you can define a conditional symbol using the <conditionalSymbol> tag. A conditional symbol represents a value that is acquired by evaluation a series of condition expressions. If any expression returns `true`, Request Mapper uses the member to calculate the return value. When a member meets the condition expression, Request Mapper evaluates a corresponding return expression, and return the result. After finding a result to return, Request Mapper does not evaluate any further expressions.

Within the <conditionalSymbol> tag, use the following tags.

<name>
The name of the symbol. It is a string and must start with the $ character.

<type>
The type of the value that the symbol returns. Specify this value as a fully qualified Java class name, or a Java primitive. Specifying the type for the symbol is optional. If it is not defined, the Request Mapper attempts to establish the field type based on the expression. If the Request Mapper is unable to determine the symbol type before evaluating the expression, performance is affected. Therefore, for best performance, it is better to specify the type.

<args>
The arguments for the symbol. This tag is optional; if it is specified, arguments must be supplied for evaluating the symbol. For more information, see "Defining symbol arguments" on page 341.

<if condition="*expression*">
The `condition` attribute defines a condition expression to evaluate. The expression must yield a Boolean value. If the value is `true`, Request Mapper uses the contents of the <if> tag to try to determine the return value. The <if> tag must contain either, but not both, of the following contents:

- A <return> tag. This tag contains an expression. If the condition expression is true, Request Mapper evaluates the expression and returns the result.
- Any number of <if> tags, nested within this <if> tag. If the condition expression is true, Request Mapper processes the nested <if> tags in the same way as a top-level <if> tag. That is, it evaluates the expression in the `condition` attribute, and if the expression is true, uses the contents of the tag to try and determine the return value.

Important: If a return value is determined, Request Mapper does not evaluate any further expressions. However, if a condition expression in an <if> tag is true, but it contains nested <if> tags and none of their condition expressions are true, no value is determined. In this case, Request Mapper continues to evaluate subsequent expressions.

<defaultValue>
Optional. If Request Mapper has evaluated all condition expressions, but none of the condition expression has returned `true`, Request Mapper evaluates the expression in the <defaultValue> tag. The conditional symbol returns the value that the expression produces. If this tag is not present, the default value is `null`.

Example

```
<symbol>
  <name>$GET</name>
  <eval>"GET"</eval>
</symbol>
<symbol>
  <name>$PUT</name>
  <eval>"PUT"</eval>
</symbol>
<conditionalSymbol>
  <name>$sessionAttribute</name>
  <if condition="$httpServletRequest.getSession(false) != null>
     <if condition="$httpServletRequest.getSession(false).getAttribute($GET)
!= null">
       <return>$httpServletRequest.getSession(false).getAttribute($GET)</return>
    </if>
     <if condition="true">
```

```
       <return>$httpServletRequest.getSession(false).getAttribute($PUT)</return>
      </if>
  </if>
</conditionalSymbol>
```

This symbol is assumed to be a part of the Servlet request mapper. First it checks if an HTTP session exists for the servlet; if not, the symbol returns `null`. If a session is present, the symbol checks if the Servlet has an attribute "GET", it returns the value of that attribute. Otherwise, it returns the value of the "PUT" attribute. The second condition expression is "true"; this value is used as an "else" clause. If the first condition is true, Request Mapper does not evaluate any further expressions; otherwise it continues to the second expression.

Defining external class symbols

Within the <symbolDefinitions> tag, you can define an external class using the <externalClassSymbol> tag. An external class symbol represents an external Java class. External class symbol definition is optional; you can use external Java classes in expressions directly. However, it might enhance the readability of the Request Mapper configuration.

Within the <externalClassSymbol> tag, use the following tags.

`<name>`
The name of the symbol. It is a string and must start with the $ character.

`<className>`
The name of the customer defined class.

Important: To refer to any Java class in Request Mapper configuration, whether in an external class symbol definition or in any expression, you must add the full path and name of the JAR file containing the class to the <requestMapperClassPath> tag within the <runtimeConfiguration> tag.

After defining an external symbol, you can refer to the class by the name of the symbol. You can also refer to static methods and fields of the class using the symbol.

Example

```
<externalClassSymbol>
  <name>$rand</name>
  <className>user.class.Random</className>
</externalClassSymbol>
```

This symbol refers to a user-written class, generating a random number. The full path and name of the JAR file containing this class must be present in the <requestMapperClassPath> tag within the <runtimeConfiguration> tag.

To refer to the static method `user.class.Random.generate()` in an expression, you can use the external symbol:

```
$rand.generate()
```

Mapping values to context keys

Within the <requestMapperDefinition> tag, map values to context keys using the <selection> tag. This mapping provides the changes in the monitoring information.

You can map values to the output keys defined for the request type (for more information, see Table 51 on page 348).

If no value is mapped to a key after the evaluation of the request mapper configuration, ITCAM uses the original value extracted from the request.

Within the <selection> tag, use the following tags.

<matchCriteria>
An expression that must return a Boolean value. The mapping defined within this tag is only used if this expression returns `true`.

<mapTo>
Defines a key and the value to map to it. Within this tag, a <key> tag contains the key, and a <value> tag contains the value.

<selection>
You can nest <selection> tags, placing one within another.

If <selection> tags are nested, then the nested mapping is only used if both the outer and the nested <matchCriteria> expressions return `true`.

You can use multiple <selection> tags within a <requestMapperDefinition> tag or within another <selection> tag. If the same key is mapped several times in several <selection> tags on the same nesting level (that is, within the same parent tag), then the first mapping for which the <matchCriteria> expression returned `true` is used.

Do not map the same key both in the outer and nested <selection> tags.

Typically, use the <matchCriteria> value of `true` as an "else" value for the last selection tag on a nesting level. If you want to map different values in different cases, use several <selection> tags within this outer tag; each of them can contain the criteria and values for a particular case. The last tag, with a value of `true`, covers the case when the available data meets none of the criteria.

Examples

```
<selection>
   <matchCriteria>true</matchCriteria>
   <mapTo>
      <key>Result</key>
      <value>$s1</value>
   </mapTo>
</selection>
```

In this mapping configuration, `Result` is set to the value of the symbol `$s1`.

```
<matchCriteria>true</matchCriteria>
   <selection>
      <matchCriteria>$b1</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>1</value>
      </mapTo>
   </selection>
   <selection>
      <matchCriteria>true</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>2</value>
      </mapTo>
</selection>
```

In this mapping configuration, the symbol $b1 must return a Boolean value. Result is set to 1 if $b1 returns true, and to 2 if $b1 returns false. If $b1 returns true, Request Mapper uses the mapping for Result in the first <selection> tag; the mapping for the same key in the second tag is not used.

Enabling a request mapper

To enable a request mapper for a request type, edit the toolkit custom configuration file or the toolkit global custom configuration file.

Add two lines to the toolkit_custom.properties or toolkit_global_custom.properties file:

- A line setting the enabling property for this request type (for more information, see "Request mapper type names, input, and output data") to true.
- A line setting the am.camtoolkit.gpe.customxml.* property to the name of the mapper XML (for more information, see "XML file syntax" on page 338). This file must be in the same directory as the configuration file referencing it. For example, if you reference the XML file in the *DC_home*/runtime/toolkit_global_custom.properties file, place the XML file in the *DC_home*/runtime directory. Use any unique value instead of the * symbol.

For more information about the toolkit_custom.properties or toolkit_global_custom.properties files, see "Properties files for the Data Collector" on page 321.

Example

To enable a request mapper that is defined in renameDataSource.xml for the SQL request type, add the following lines to the toolkit custom configuration file or the toolkit global custom configuration file:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

Request mapper type names, input, and output data

The following tables list the information necessary to configure and enable request mappers for different request types.

Request type
The request type.

Enabling property
To enable the request mapper, set this property to true in the toolkit_custom.properties or toolkit_global_custom.properties file.

Important: If you copy this value from the table, remove any spaces and line breaks.

Request mapper type name
Assign this value to the type attribute of the <requestMapperDefinition> tag in the request mapper definition XML file.

Input data symbol names
The symbols representing the request information. You can use these symbols in expressions within the request mapper definitions (for more information, see "Defining an expression" on page 338).

Output data context keys
To provide changes in the monitoring information, assign values to these keys in the request mapper definition. For more information, see "Mapping values to context keys" on page 345.

Table 51. Request mapper enabling properties and type names

Request type	Enabling property	Request mapper type name
Custom Request		Defined by user in the edgeRequest definition
JAX-RPC Web Service	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`
Axis Web Service	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`
JAX-WS Web Service	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`

Important: In ITCAM for SOA, there is no meaningful way to configure the custom request mapper for the request types not listed in Table 51.

Table 52. Request mapper input and output data

Request type	Input data symbol names	Output data context keys
JAX-RPC Web Service	• **$messageContext** the IMessageContextWrapper • **$appName** the application name • **$requestName** the default request name • **$url** the URL • **$context** indicates the type of request: "WebServicesJaxRpc ProviderRequest", "WebServicesJaxRpc ClientRequest"	**appName** the renamed application name **requestName** the renamed request name **url** the renamed URL
Axis Web Service	• **$messageContext** the IMessageContextWrapper • **$appName** the application name • **$requestName** the default request name • **$url** the URL • **$context** indicates the type of request: "WebServicesAxisClient Request", "WebServicesAxis ProviderRequest"	**appName** the renamed application name **requestName** the renamed request name **url** the renamed URL
JAX-WS Web Service	• **$messageContext** the IMessageContextWrapper • **$appName** the application name • **$requestName** the default request name • **$url** the URL • **$context** indicates the type of request: "WebServicesJAXWS ClientRequest", "WebServicesJAXWS ProviderRequest", "WebServicesJAXWS AsyncRequest"	**appName** the renamed application name **requestName** the renamed request name **url** the renamed URL

Example request mapper definitions

The following examples illustrate usage of the request mapper functionality.

Changing the servlet application name

In this example, the application name in a servlet request is replaced by the URI and the query string.

The *DC_home*/runtime/changeAppname.xml file contains the following request mapper definition:

```
<gpe>
   <runtimeConfiguration>
         <requestMapperDefinition type="servlet">
               <selection>
                      <matchCriteria>true</matchCriteria>
                      <mapTo>
                             <key>appName</key>
                             <value>$URI + "." + $QueryString</value>
                      </mapTo>
               </selection>
         </requestMapperDefinition>
   </runtimeConfiguration>
</gpe>
```

Renaming a data source

In this example, the data source name in an SQL request is changed to a version that a user can understand more easily.

The *DC_home*/runtime/renameDataSource.xml file contains the following request mapper definition:

```
<gpe>
 <runtimeConfiguration>
   <requestMapperDefinition type="sqlStatement">
      <selection>
         <matchCriteria>$dataSourceName != null</matchCriteria>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/TradeDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Daytrader Data Source"</value>
           </mapTo>
         </selection>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/LongDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Long term trader Data Source"</value>
           </mapTo>
         </selection>
      </selection>
   </requestMapperDefinition>
 </runtimeConfiguration>
<gpe>
```

The first <selection> tag ensures that `$dataSourceName` is not null. Then the second <selection> tag can safely evaluate `$dataSourceName.equals()`.

If the first <selection> tag was not present, and a null `$dataSourceName` was passed, the request mapper would generate an exception. Such an exception might result in missing monitoring information.

To enable this request mapper, the file *DC_home*/runtime/toolkit_global_custom.properties contains the following lines:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

Removing sensitive information from an SQL request

In this example, an application includes social security numbers in SQL requests. The request mapper removes the numbers from the version of the request that the user can see.

In the SQL requests, the social security number is listed with the SS column name: `SS = *number*`. The request mapper looks for the string "SS = " and removes the nine symbols after it.

The *DC_home*/runtime/removeSSN.xml file contains the following request mapper definition:

```
<gpe>
    <runtimeConfiguration>
         <requestMapperDefinition type="sqlStatement">
             <symbolDefinitions>
                 <symbol>
                     <name>$offsetOfSS</name>
                     <eval>$sqlText.indexOf("SS = ")</eval>
                 </symbol>
                 <symbol>
                     <name>$sqlTextContainsSS</name>
<eval>$sqlText != null AND $offsetOfSS > 0 AND $sqlText.length() GE
$offsetOfSS+16</eval>
                 </symbol>
                 <conditionalSymbol>
                     <name>$sqlTextPriorToSSKeyword</name>
                     <type>java.lang.String</type>
                     <defaultValue>""</defaultValue>
                     <if condition="$sqlTextContainsSS">
                       <return>$sqlText.substring(0, $offsetOfSS+5)</return>
                     </if>
                 </conditionalSymbol>
                 <conditionalSymbol>
                     <name>$sqlTextAfterSS</name>
                     <type>java.lang.String</type>
                     <defaultValue>""</defaultValue>
                     <if condition="$sqlTextContainsSS">
                       <return>$sqlText.substring($offsetOfSS+16)</return>
                     </if>
                 </conditionalSymbol>
             </symbolDefinitions>
             <selection>
                  <matchCriteria>$sqlText != null AND $sqlText.length() >
0</matchCriteria>
                  <selection>
                       <matchCriteria>$sqlTextContainsSS</matchCriteria>
                       <mapTo>
                            <key>sqlText</key>
                            <value>$sqlTextPriorToSSKeyword + "?" +
$sqlTextAfterSS</value>
                       </mapTo>
                  </selection>
             </selection>
         </requestMapperDefinition>
    </runtimeConfiguration>
</gpe>
```

To enable this request mapper, the file *DC_home*/runtime/toolkit_global_custom.properties contains the following lines:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=removeSSN.xml
```

Starting and stopping the monitoring environment

Procedures are provided for starting and stopping various components, databases, and application servers associated with ITCAM Data Collector for WebSphere.

Disabling and re-enabling a data collector

If you want to disable a data collector without unconfiguring or uninstalling it, complete the following procedure:

1. Log in to the IBM WebSphere Application Server administrative console.
2. Expand **Servers > Server Type** and click **WebSphere application servers**.
3. Choose the *server_name*.
4. On the Configuration tab, under the **Server Infrastructure** section, expand **Java and Process Management** and select **Process Definition**.
5. Under the **Additional Properties** section, go to **Java Virtual Machine > Custom Properties**.
6. Find a property with the name `ITCAM_DC_ENABLE`. If this property is not present, add it.
7. Set the value of this property to `false`.
8. Click **OK** or **Apply**. Click **Save**.
9. Restart the application server (for more information, see "Restarting the application server")

To re-enable a data collector that was disabled in this way, complete the following procedure:

1. Log in to the IBM WebSphere Application Server administrative console.
2. Expand **Servers > Server Type** and click **WebSphere application servers**
3. Choose the *server_name*.
4. On the Configuration tab, under the **Server Infrastructure** section, expand **Java and Process Management** and select **Process Definition**.
5. Under the **Additional Properties** section, go to **Java Virtual Machine > Custom Properties**.
6. Find the property with the name `ITCAM_DC_ENABLE`.
7. Set the value of this property to `true`.
8. Click **OK** or **Apply**. Click **Save**.
9. Restart the application server (for more information, see "Restarting the application server")

Restarting the application server

There are separate procedures for restarting the application server in a Network Deployment and non-Network Deployment environments.

Restarting the application server in a non-Network Deployment

To restart the application server, complete the following steps:

Table 53. Restarting the application server

Platform	Steps

Windows	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere >** ***application_server_and_version*>** **Profiles >** ***profile_name*** **> First steps**.
	2. Click **Stop the server**.
	Wait for the First steps output window to display a message similar to the following message:
	`Server` *`server_name`* `stop completed`
	3. Click **Start the server**.
	The First steps output window displays a message that is similar to the following message:
	`Server` *`server_name`* `open for e-business`
	• From a command line:
	`cd` *`AppServer_home`*`\profiles\`*`profile_name`*`\bin`
	`stopServer` *`server_name`* `[options]`
	`startServer` *`server_name`*

Linux or UNIX systems	`cd` *`AppServer_home`*`/profiles/`*`profile_name`*`/bin`
	`./stopServer` *`server_name`* `[options]`
	`./startServer` *`server_name`*

The *`server_name`* is the name of the configuration directory of the server that you want to restart. The default is `server1`.

The *`profile_name`* specifies the profile name. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *`name`* or `-user` *`name`* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Restarting the application server in a Network Deployment environment

To restart the application server, complete the following steps:

1. Change to the *`AppServer_home`*`/bin` directory.
2. Stop all servers that are on the node, and the node itself. Run the `stopNode -stopservers` command
3. Stop the deployment manager process. Run the `stopManager` command.
4. Start the deployment manager process. Run the `startManager` command.
5. Start the node. Run the `startNode` command.

6. For each application server on the node, start the application server using the procedure in "Starting the application server in a non-Network Deployment environment."

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Starting the application server

There are separate procedures for starting the application server in a Network Deployment and non-Network Deployment environments.

Starting the application server in a non-Network Deployment environment

To start the application server, complete the following steps:

Table 54. Starting the application server.

Platform	**Steps**

Windows systems	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere >** ***application_server_and_version*>** **Profiles >** ***profile_name*** **> First steps**.
	2. Click **Start the server**.
	The First steps output window displays a message that is similar to the following message:
	`Server` *`server_name`* `open for e-business`
	• From a command line:
	`cd` *`AppServer_home`*`\profiles\`*`profile_name`*`\bin`
	`startServer` *`server_name`*

Linux or UNIX systems	`cd` *`AppServer_home`*`/profiles/`*`profile_name`*`/bin`
	`./startServer` *`server_name`*

The *`server_name`* is the name of the configuration directory of the server that you want to start. The default is `server1`.

The *`profile_name`* specifies the profile name for the application servers. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.

- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Starting the application server in a Network Deployment environment

To start the application server, complete the following steps:

1. Change to the *`AppServer_home`*`/bin` directory.
2. Start the deployment manager process. Run the `startManager` command.
3. Start the node. Run the `startNode` command.
4. For each application server on the node, start the application server using the procedure in "Starting the application server in a non-Network Deployment environment" on page 353.

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *`name`* or `-user` *`name`* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *`password`* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Stopping the application server

There are separate procedures for stopping the application server in Network Deployment and non-Network Deployment environments.

Stopping the application server in a non-Network Deployment environment

Complete the following steps to stop the application server:

Table 55. Stopping the application server.

Platform	**Steps**

Windows	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere >** ***application_server_and_version*>** **Profiles >** ***profile_name*** **> First steps**.
	2. Click **Stop the server**.
	Wait for the First steps output window to display a message that is similar to the following message:
	`Server` *`server_name`* `stop completed`
	• From a command line:
	`cd` *`AppServer_home`*`\profiles\`*`profile_name`*`\bin`
	`stopServer` *`server_name`* `[options]`

Table 55. Stopping the application server. (continued)

Platform	Steps

Linux or UNIX systems	`cd AppServer_home/profiles/profile_name/bin`
	`./stopServer server_name [options]`

The *server_name* is the name of the configuration directory of the server that you want to stop. The default is `server1`.

The *profile_name* specifies the profile name for the application servers. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Stopping the application server in a Network Deployment environment

Complete following steps to stop the application server:

1. Change to the *AppServer_home*/`bin` directory.
2. Stop all servers that are on the node, and the node itself. Run the `stopNode -stopservers` command
3. Stop the deployment manager process. Run the `stopManager` command.

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Part 3. Configuring data collector for WebSphere Message Broker environments

After you run the installation program to install application support for Tivoli Monitoring components, you run the installation wizard to install the ITCAM for SOA monitoring agent. During the installation of the monitoring agent, you choose to install Data Collector for WebSphere Message Broker.

When you install the data collector, a configuration utility is provided for configuring data collection for WebSphere Message Broker environments.

This part of the *IBM Tivoli Composite Application Manager for SOA Installation Guide* describes the procedures for configuring Data Collector for WebSphere Message Broker.

Chapter 9. Configuring data collection: WebSphere Message Broker

ITCAM for SOA provides support for data collection in IBM WebSphere Message Broker environments.

The list of versions of WebSphere Message Broker supported by ITCAM for SOA is available from the Software product compatibility reports website. For information about accessing reports from this website, see "Required software" on page 15.

Refer to your IBM WebSphere Message Broker documentation for procedures on installing or upgrading to the minimum supported versions.

Beginning with ITCAM for SOA version 7.2 Fix Pack 1, a new data collector, Data Collector for WebSphere Message Broker, is provided for monitoring WebSphere Message Broker environments. The data collector is a shared component of ITCAM for Transactions version 7.3 or later and ITCAM for SOA version 7.2 Fix Pack 1 and later.

To install the data collector, install the Data Collector for WebSphere Message Broker component as part of either an ITCAM for SOA or ITCAM for Transactions installation. When prompted by the installer, select the Tivoli Enterprise Monitoring Agent Framework and the Data Collector for WebSphere Message Broker components.

Restriction: When you install the agent on a remote system from the Tivoli Enterprise Portal or using `tacmd` commands, the Data Collector for WebSphere Message Broker is not installed. To install the Data Collector for WebSphere Message Broker on a remote system, copy the ITCAM for SOA installation media to the remote system, run the installation wizard, and select the Data Collector for WebSphere Message Broker from the list of features that are available for installation.

A new configuration utility, Data Collector for WebSphere Message Broker `configDC` utility, is provided for enabling the `KK3UserExit`. Modify the `KK3.dc.properties` to start data collection.

If the data collector is installed and is at the same maintenance level, skip the steps to install and enable the data collector. Instead, integrate the data collector with the ITCAM for SOA monitoring agent by setting the `default.kd4.enabled` property in the `KK3.dc.properties` properties file to `true`. The `KK3.dc.properties` file is in the *MB_dc_home* `config` directory. For more information about integrating the data collector with ITCAM for SOA, see "Integrating the data collector with ITCAM for SOA and ITCAM for Transactions" on page 368.

After you configure your WebSphere Message Broker environment for data collection, see the *IBM Tivoli Composite Application Manager for SOA User's Guide* for information about displaying WebSphere Message Broker data in service-to-service topology views.

Table 56 lists the inter-domain tracking that is supported by Data Collector for WebSphere Message Broker, when the data collector is integrated with ITCAM for Transactions:

Table 56. Domain tracking that is supported

Domain interactions that are tracked	Comments
• WebSphere Message Broker to WebSphere MQ • WebSphere MQ to WebSphere Message Broker	Requires MQ tracking
• WebSphere Message Broker to Microsoft .NET • Microsoft .NET to WebSphere Message Broker	Requires .NET Data Collector Tracks SOAP only
• WebSphere Message Broker to IBM HTTP Server	Requires Application Response Measurement (ARM) Tracks HTTP only
• WebSphere Message Broker to WebSphere Application Server • WebSphere Application Server to WebSphere Message Broker	Requires either of the following products: • WebSphere Application Server data collector that is installed as part of ITCAM for Application Diagnostics V7.1 • ITCAM Data Collector for WebSphere Applications that is installed as part of ITCAM for Applications V7.2 Tracks SOAP only

Upgrading to the Data Collector for WebSphere Message Broker

If you installed any of the following components in your environment, you might have enabled data collection for WebSphere Message Broker using an older version of the data collector:

- ITCAM for SOA version 7.2
- ITCAM for Transactions version 7.2 Fix Pack 1 or earlier

The `upgradeBrokers` script is provided to upgrade the older versions of the data collector. When you enable data collection, if the `configDC` utility detects that an older version of the data collector exists, it prompts you to run the `upgradeBrokers` script.

Important: You must enable data collection using the `configDC` utility before you run the `upgradeBrokers` script.

Restriction: If the `configDC` utility detects that an older version of an ITCAM for SOA data collector and an older version of the ITCAM for Transactions data collector exists, you cannot use the `upgradeBrokers` script to migrate the data collectors. Instead, you must manually remove the `TTDCUserExit` and `MqsiSOAExit` (see “Manually remove TTDCUserExit or MqsiSOAExit user exits” on page 363).

Upgrading an ITCAM for SOA version 7.2 data collector to Data Collector for WebSphere Message Broker

To upgrade an ITCAM for SOA WebSphere Message Broker data collector, complete the following general procedure:

1. Verify that you installed ITCAM for SOA version 7.2 or upgraded to ITCAM for SOA version 7.2.
2. Update the ITCAM for SOA monitoring agent to ITCAM for SOA version 7.2 Fix Pack 1 and install the Data Collector for WebSphere Message Broker. For more information, see “Installing and upgrading the ITCAM for SOA monitoring agent and data collectors” on page 40 on Windows systems or “Installing, upgrading, and updating the monitoring agents and data collectors” on page 81 on Linux or AIX systems.
3. The installer detects that the ITCAM for SOA agent is installed and integrates the Data Collector for WebSphere Message Broker with the ITCAM for SOA agent. The installer sets the `default.kd4.enabled` property in the Data Collector for WebSphere Message Broker properties file, `KK3.dc.properties`, to `true`.
4. Close any Websphere Message Broker command consoles that are open.
5. Navigate to the *MB_DC_home*`\bin` directory.
6. Start the `configDC` utility to enable data collection by issuing the following command:

   ```
   configDC.bat -enable broker_installation_directory
   ```

   For example, on Windows systems:

   ```
   C:\IBM\ITM\TMAITM6\k3\bin\configDC.bat -enable C:\IBM\mqsi\7.0
   ```

   On Linux and AIX systems:

   ```
   /opt/IBM/ITM/aix513/k3/bin/configDC.sh -enable /opt/IBM/mqsi/7.0
   ```
7. The `configDC` utility detects that a user exit for a previous version of an ITCAM for SOA WebSphere Message Broker data collector is configured. The utility prompts you to run the `upgradeBrokers` script. This script is used to migrate the older versions of the user exits (`MqsiSOAExit`) to the user exits that are provided with the Data Collector for WebSphere Message Broker.
8. Before running the `upgradeBrokers` script, restart any MQSI command prompts or shells and load the MQSI environment for the broker installation that you want to upgrade:
   a. On Windows systems, select the Command console shortcut from the WebSphere Message Broker start menu.
   b. On Linux and AIX systems, run the `mqsiprofile` script that is in the WebSphere Message Broker installation `bin` directory. For example:

      ```
      . /opt/ibm/mqsi/7.0/bin/mqsiprofile
      ```
9. From the *MB_DC_home* `bin` directory, run the `upgradeBrokers` script by issuing the following command:

   ```
   upgradeBrokers.bat -silent broker_name1 broker_name2
   ```

   Separate multiple broker names with a space. For example, on Windows systems:

   ```
   C:\IBM\ITM\TMAITM6\k3\bin\upgradeBrokers.bat -silent broker1 broker2
   ```

   On Linux and AIX systems:

   ```
   /opt/IBM/ITM/aix513/k3/bin/upgradeBrokers.sh -silent broker1 broker2
   ```
10. When all brokers on the computer system are upgraded, remove `KD4setupSOAUserExitPath` from the `$MQSI_WORKPATH/common/profiles` directory.
11. Copy the following settings in the `KD4.dc.properties` file to the `KK3.properties` file if the properties are not already set:

```
default.tt.enabled
default.tt.serverstring
default.ttdc.mq.installdir
```

The properties files are in the following locations:

- The `KD4.dc.properties` file is in the `ITCAM4SOA_HOME\KD4\config` directory on Windows systems and in the `ITCAM4SOA_HOME/KD4/config` directory on Linux and AIX systems.
- The `KK3.properties` properties file is in the *`MB_dc_home`*`\config` directory on Windows systems and in the *`MB_dc_home`*`/config` on Linux and AIX systems.

Upgrading an ITCAM for Transactions version 7.2.0.2 or earlier data collector to Data Collector for WebSphere Message Broker

When you update to ITCAM for SOA version 7.2 Fix Pack 1, you might not have already configured data collection for WebSphere Message Broker using the ITCAM for SOA data collector. However, you might have WebSphere Message Broker Tracking configured in your environment as part of an ITCAM for Transactions version 7.2.0.2 or earlier installation.

You must upgrade WebSphere Message Broker Tracking to Data Collector for WebSphere Message Broker if you want to configure data collection for WebSphere Message Broker.

To upgrade to the Data Collector for WebSphere Message Broker, complete the following steps:

1. Install the ITCAM for SOA monitoring agent version 7.2.
2. Update the ITCAM for SOA monitoring agent to ITCAM for SOA version 7.2 Fix Pack 1 and install the Data Collector for WebSphere Message Broker. For more information, see “Installing and upgrading the ITCAM for SOA monitoring agent and data collectors” on page 40 on Windows systems or “Installing, upgrading, and updating the monitoring agents and data collectors” on page 81 on Linux or AIX systems.
3. The installer detects that WebSphere Message Broker Tracking is installed. The installer migrates the following settings to the `KK3.dc.properties` file:
   - `default.tt.enabled`
   - `default.tt.serverstring`
   - `default.ttdc.mq.installdir`
   - `default.log`
   - `default.trace`
   - `default.operations.count`
   - `default.operations.size`
   - `default.trace.count`
   - `default.trace.size`
4. Close any Websphere Message Broker command consoles that are open.
5. Navigate to the *`MB_DC_home`*`\bin` directory.
6. Start the `configDC` utility to enable data collection by issuing the following command:

   ```
   configDC.bat -enable broker_installation_directory
   ```

   For example, on Windows systems:

   ```
   C:\IBM\ITM\TMAITM6\k3\bin\configDC.bat -enable C:\IBM\mqsi\7.0
   ```

On Linux and AIX systems:

```
/opt/IBM/ITM/aix513/k3/bin/configDC.sh -enable /opt/IBM/mqsi/7.0
```

7. The `configDC` utility detects that a user exit for a previous version is configured. The utility prompts you to run the `upgradeBrokers` script. The script migrates the older versions of the user exits (`TTDCUserExit`) to the user exits that are provided with the Data Collector for WebSphere Message Broker.
8. Before running the `upgradeBrokers` script, restart any MQSI command prompts or shells and load the MQSI environment for the broker installation that you want to upgrade:
   a. On Windows systems, select the Command console shortcut from the WebSphere Message Broker start menu.
   b. On Linux and AIX systems, run the `mqsiprofile` script that is in the WebSphere Message Broker installation bin directory. For example:
   ```
   . /opt/ibm/mqsi/7.0/bin/mqsiprofile
   ```
9. From the *MB_DC_home* `bin` directory, run the `upgradeBrokers` script by issuing the following command:
   ```
   upgradeBrokers.bat -silent broker_name1 broker_name2
   ```

   Separate multiple broker names with a space. For example, on Windows systems:
   ```
   C:\IBM\ITM\TMAITM6\k3\bin\upgradeBrokers.bat -silent broker1 broker2
   ```

   On Linux and AIX systems:
   ```
   /opt/IBM/ITM/aix513/k3/bin/upgradeBrokers.sh -silent broker1 broker2
   ```
10. Integrate the data collector with the ITCAM for SOA monitoring agent. For more information, see “Integrating the data collector with ITCAM for SOA and ITCAM for Transactions” on page 368.
11. When all brokers on the computer system are upgraded, remove the script files from the `$MQSI_WORKPATH/common/profiles` directory. The files set the `MQSI_USER_EXIT_PATH` environment variable to point to the installation directory of `TTDCUserExit`.

Manually remove `TTDCUserExit` or `MqsiSOAExit` user exits

If the `configDC` utility detects that an older version of the ITCAM for SOA data collector and an older version of the ITCAM for Transactions data collector exists, you must manually remove the user exits of the previous version of the data collectors. The `configDC` utility warns you of the presence of both types of user exits with a message similar to the following:

```
Message Broker Tracking (the TTDCUserExit) has been detected
in ttdcInstallDirectory and an older version of
ITCAM for SOA data collection for WebSphere Message Broker (the MqsiSOAExit)
has been detected
 in soaInstallDirectory. Please restart all
MQSI command shells and use the mqsichangebroker
 and mqsichangeflowuserexits commands to upgrade the broker user
 exits from MqsiSOAExit and TTDCUserExit to KK3UserExit.
```

To manually remove the user exits, complete the following steps for each broker that you need to upgrade:

1. Verify that the broker is running by issuing the `mqsilist` *broker_name* command. For example, on Windows systems:

```
C:\Program Files\IBM\MQSI\8.0>mqsilist bk1
----------------------------------
BIP1286I: Execution group 'eg1' on broker 'bk1' is running.
BIP8071I: Successful command completion.
```

On Linux and AIX systems:

```
[root@ppc01 config]# mqsilist bk1
BIP8130I: Execution Group: eg1  -  20401
<-This number is 0 if the broker is not running
BIP8071I: Successful command completion.
```

2. Update the active user exits for the broker:
   a. List the active user exits for the broker by issuing the **mqsireportflowuserexits** command:

      ```
      mqsireportflowuserexits broker_name
      ```

   b. If one of the user exit names TTDCUserExit or MqsiSOAExit, or both, are present in the active user exit list, replace the exit names in the list with KK3UserExit and issue the **mqsichangebroker** command to reset the active user exits:

      ```
      mqsichangebroker broker_name –e newActiveUserExitsList
      ```

3. Update the user exits for execution groups:
   a. List the execution groups that are configured for the broker:

      ```
      mqsilist broker_name
      ```

   b. List the active and inactive user exits for each execution group:

      ```
      mqsireportflowuserexits broker_name –e executionGroupName
      ```

   c. If one of the user exit names TTDCUserExit, or MqsiSOAExit, or both, are present in either user exit list, replace the exit names in the lists with KK3UserExit and issue the **mqsichangebroker** command to reset the user exits:

      ```
      mqsichangebroker brokerName –e executionGroupName
      -a newActiveUserExitsList
      -i newInactiveUserExitsList
      ```

4. Update the user exits for message flows:
   a. List the message flows that are configured for each execution group:

      ```
      mqsilist broker_name –e executionGroupName
      ```

   b. Check the active and inactive user exits for message flows:

      ```
      mqsireportflowuserexits broker_name –e executionGroupName
      –f messageFlowName
      ```

   c. If one of the user exit names TTDCUserExit, or MqsiSOAExit, or both, are present in the user exit list, replace the exit names in the lists with KK3UserExit and issue the **mqsichangebroker** command to reset the user exits:

      ```
      mqsichangebroker brokerName –e executionGroupName
      –f messageFlowName -a newActiveUserExitsList
      -i newInactiveUserExitsList
      ```

Update the maintenance level of the data collector

To install a new maintenance version of Data Collector for WebSphere Message Broker, complete the following steps:

1. Install the new version of the Data Collector for WebSphere Message Broker.
2. Stop the broker instance using the mqsistop *broker_name* command. For example:

   ```
   mqsistop MB8BROKER
   ```

3. Load the KK3UserExit user exit library for a WebSphere Message Broker installation by issuing the following command:

   ```
   configDC -enable broker_installation_directory
   ```

   For example, on Windows systems:

   ```
   C:\IBM\ITM\TMAITM6\k3\bin\configDC.bat -enable C:\IBM\mqsi\7.0
   ```

   On AIX systems:

   ```
   /opt/IBM/ITM/aix513/k3/bin/configDC.sh -enable /opt/IBM/mqsi/8.0.0.0
   ```

   On Linux systems:

   ```
   /opt/IBM/ITM/ls3263/k3/bin/configDC.sh -enable /opt/IBM/mqsi/8.0.0.0
   ```
4. Restart the broker instance using the mqsistart *broker_name* command. For example:

   ```
   mqsistart MB8BROKER
   ```

WebSphere Message Broker configuration utility

Use the ConfigDC utility to configure the WebSphere Message Broker environment to load the KK3UserExit for the Data Collector for WebSphere Message Broker.

The ConfigDC utility is in the *MB_dc_home*\bin directory on Windows systems and in the *MB_dc_home*/bin directory on Linux and UNIX systems. The utility can be run in console mode. The utility cannot be run in the graphical user interface mode or silent mode.

The command options for the ConfigDC utility are as follows:

-enable
Configures the environment to load the KK3UserExit.

-disable
Removes the KK3UserExit from the environment.

broker_installdir
(Optional) WebSphere Message Broker installation directory. If broker_install_dir is not specified, the Data Collector for WebSphere Message Broker checks for $MQSI_WORKPATH to determine whether to load the KK3UserExit for the current broker installation or all installations.

Enabling data collection

Before you enable data collection, you must install Data Collector for WebSphere Message Broker as part of an ITCAM for SOA or an ITCAM for Transactions installation.

To enable data collection for a WebSphere Message Broker environment, enable the KK3UserExit for all message flows to be monitored. The KK3UserExit can be enabled for individual message flows, or it can be enabled for an entire WebSphere Message Broker instance.

To enable data collection for a WebSphere Message Broker environment on a Windows system, complete the following steps:

1. Verify that the user has sufficient permissions to write to the C:\Documents and Settings\All Users\Application Data\IBM\MQSI\common\profiles directory.
2. Close any Websphere Message Broker command consoles that are open.

3. Navigate to the *MB_DC_home*\bin directory.
4. Load the KK3UserExit user exit library for a WebSphere Message Broker installation by issuing the following command:

   ```
   configDC.bat -enable broker_installation_directory
   ```

   For example:

   ```
   C:\IBM\ITM\TMAITM6\k3\bin\configDC.bat -enable C:\IBM\mqsi\7.0
   ```
5. Open the WebSphere Message Broker command console for your version of WebSphere Message Broker.

   Remember: You might have more than one version of WebSphere Message Broker installed on your system. Be sure to start the command console for the correct version of WebSphere Message Broker.
6. Stop the WebSphere Message Broker instances on which you want to enable data collection using the mqsistop *broker_name* command. For example:

   ```
   mqsistop MB8BROKER
   ```
7. If you want to enable KK3UserExit for all message flows on the WebSphere Message Broker instances, use the following command:

   ```
   mqsichangebroker broker_name -e "KK3UserExit"
   ```

   For example:

   ```
   mqsichangebroker MB8BROKER -e "KK3UserExit"
   ```

   Use this command to change the default state of the user exit to active for all message flows on the WebSphere Message Broker instance. If you skip this step, KK3UserExit is disabled by default for all message flows.
8. Restart the WebSphere Message Broker instances using the mqsistart *broker_name* command. For example:

   ```
   mqsistart MB8BROKER
   ```
9. If you skipped step 7 and you want to enable KK3UserExit for a specific message flow, use the following command:

   ```
   mqsichangeflowuserexits broker_name -e execution_group_name -f
   message_flow_name -a "KK3UserExit"
   ```

   For example:

   ```
   mqsichangeflowuserexits MB8BROKER -e default -f myFlow -a KK3UserExit
   ```

   To specify multiple user exists, use a colon-separated list. For example:

   ```
   mqsichangeflowuserexits MB8BROKER -e default -f myFlow -a
   KK3UserExit:exit2:exit3
   ```

Data collection is enabled for the specified message flows on the WebSphere Message Broker.

To enable data collection for a WebSphere Message Broker environment on a Linux or AIX system, complete the following steps:

1. Verify that the user has sufficient permissions to write to the /var/mqsi/common/profiles directory.
2. Close any Websphere Message Broker shells that have loaded the MQSI environment.
3. Navigate to the *MB_DC_home*/bin directory.

4. Issue the following command to load the KK3UserExit user exit library for a WebSphere Message Broker installation:

   ```
   ./configDC.sh -enable broker_installation_directory
   ```

   For example, on AIX systems:

   ```
   /opt/IBM/ITM/aix513/k3/bin/configDC.sh -enable /opt/IBM/mqsi/8.0.0.0
   ```

   For example, on Linux systems:

   ```
   /opt/IBM/ITM/ls3263/k3/bin/configDC.sh -enable /opt/IBM/mqsi/8.0.0.0
   ```

   Remember:

   - You might have multiple versions of WebSphere Message Broker installed on your system. Be sure to source the correct profile in your shell. Make sure only to source one profile, as sourcing multiple profiles can lead to unexpected results.
   - If the utility detects that a previous version of the data collector is configured, you must upgrade the data collector after you enable data collection. For more information, see "Upgrading to the Data Collector for WebSphere Message Broker" on page 360.
5. Ensure that the WebSphere Message Broker profile is in your shell profile, or source it manually by issuing the **mqsiprofile** command from the bin directory of the WebSphere Message Broker installation. For example:

   ```
   . /opt/ibm/mqsi/8.0.0.0/bin/mqsiprofile
   ```
6. Stop the WebSphere Message Broker instances on which you want to enable data collection using the mqsistop *broker_name* command. For example:

   ```
   mqsistop MB8BROKER
   ```
7. If you want to enable KK3UserExit for all message flows on the WebSphere Message Broker instances, use the following command:

   ```
   mqsichangebroker broker_name -e KK3UserExit
   ```

   For example:

   ```
   mqsichangebroker MB8BROKER -e KK3UserExit
   ```

   Use this command to change the default state of the user exit to active for all message flows on the WebSphere Message Broker instance. If you skip this step, KK3UserExit is disabled by default for all message flows.
8. Restart the WebSphere Message Broker instances using the mqsistart *broker_name* command. For example:

   ```
   mqsistart MB8BROKER
   ```
9. If you skipped step 7 and you want to enable KK3UserExit for a specific message flow on the WebSphere Message Broker instance, use the following command:

   ```
   mqsichangeflowuserexits broker_name -e execution_group_name -f
   message_flow_name -a KK3UserExit
   ```

   For example:

   ```
   mqsichangeflowuserexits MB8BROKER -e default -f myFlow -a KK3UserExit
   ```

   To specify multiple user exists, use a colon-separated list. For example:

   ```
   mqsichangeflowuserexits MB8BROKER -e default -f myFlow -a
   KK3UserExit:exit2:exit3
   ```

Data collection is enabled for the specified message flows on the WebSphere Message Broker.

You must modify the KK3.dc.properties file to integrate the data collector with either ITCAM for SOA or ITCAM for Transactions to start data collection. For information about starting data collection, see "Integrating the data collector with ITCAM for SOA and ITCAM for Transactions."

Integrating the data collector with ITCAM for SOA and ITCAM for Transactions

To integrate the data collector with the ITCAM for SOA monitoring agent or ITCAM for Transactions monitoring agent, or both, you must modify the contents of the KK3.dc.properties file. To modify the file, complete the following steps:

1. Navigate to the *MB_dc_home*\config directory on Windows systems or the *MB_dc_home*/config directory on Linux or AIX systems.
2. Open the KK3.dc.properties file in a text editor.

The properties file is reloaded whenever it is updated. To apply the settings in the properties file to all execution groups in a WebSphere Message Broker instance, use the prefix default. For example, to enable data collection, use default in the following property:

```
# Enable monitoring for all execution groups
default.monitor=on
```

To integrate the data collector with the ITCAM for SOA monitoring agent, complete the following steps:

1. Enable data collection. For example:
   ```
   default.monitor=on
   ```
2. Integrate the data collector with the ITCAM for SOA monitoring agent. For example:
   ```
   default.kd4.enabled=true
   ```

To integrate the data collector with the ITCAM for Transactions, complete the following steps:

1. Enable data collection. For example:
   ```
   default.monitor=on
   ```
2. Enable data to be sent to the Transaction Collector in ITCAM for Transactions. For example:
   ```
   default.tt.enabled=true
   ```
3. Specify the address of the Transaction Collector by setting the following property:
   ```
   default.tt.serverstring=transaction_collector_address
   ```

   Set the *transaction_collector_address* in the format of tcp:hostname_or_IP_address:port. For example:
   ```
   default.tt.serverstring=tcp:127.0.0.1:5455
   ```
4. Specify the directory to integrate with MQ Tracking in ITCAM for Transactions by setting the following property:
   ```
   default.ttdc.mq.installdir=path_to_MQTracking_installation_directory
   ```

   For example: default.ttdc.mq.installdir=C:\IBM\ITM\TMAITM6\kth on Windows systems or /opt/IBM/WMB/aix533/th on AIX systems.

The data collector produces an operator log with diagnostic messages. You can set the logging level to `info`, `warn`, or `error` by setting the following property:

```
default.log=info
```

The data collector can produce trace logs for L3 support, if required. You can turn on trace logs by setting the following property:

```
default.trace=on
```

Enable trace logs only when troubleshooting problems.

When the data collector is integrated with the ITCAM for SOA monitoring agent, the settings for monitor, log, and trace files are ignored. The settings are overwritten by settings that are controlled by the ITCAM for SOA agent. The settings are configured on a per-execution group basis. View these settings in the ITCAM for SOA Service Management workspace. Use the ITCAM for SOA take action commands to modify the settings.

Disabling data collection

To disable data collection for a WebSphere Message Broker environment in a Windows system, complete the following steps:

1. Open the WebSphere Message Broker command console for your version of WebSphere Message Broker.

   Remember: You might have more than one version of WebSphere Message Broker installed on your system. Be sure to start the command console for the correct version of WebSphere Message Broker.
2. If you want to disable `KK3UserExit` for a specific message flow, issue the following command:
   ```
   mqsichangeflowuserexits broker_name -e execution_group_name -f \
   message_flow_name -a ""
   ```
3. Stop the WebSphere Message Broker instances on which you want to disable data collection using the `mqistop` *broker_name* command. For example:
   ```
   mqistop MB8BROKER
   ```
4. If you skipped step 2 and you want to disable `KK3UserExit` for all message flows on the WebSphere Message Broker instance, use the following command:
   ```
   mqsichangebroker broker_name -e
   ```

   For example:
   ```
   mqsichangebroker MB8BROKER -e
   ```

   Use this command to change the current state of the user exit to inactive for all message flows on the WebSphere Message Broker instance. To disable all user exits on the WebSphere Message Broker instance, issue the following command:
   ```
   mqsichangebroker broker_name -e ""
   ```
5. Navigate to the *MB_DC_home*`/bin` directory.
6. If you disabled `KK3UserExit` for all message flows, remove the `KK3UserExit` user exit library for the WebSphere Message Broker installation by issuing the following command:
   ```
   configDC.bat -disable broker_installation_directory
   ```

   For example:
   ```
   C:\IBM\ITM\TMAITM6\k3\bin\configDC.bat -disable C:\IBM\mqsi\7.0
   ```

7. Restart the WebSphere Message Broker instances using the `mqistart` *`broker_name`* command. For example:

   ```
   mqistart MB8BROKER
   ```

Data collection is disabled for the specified message flows on the WebSphere Message Broker.

To disable data collection for a WebSphere Message Broker environment on a Linux or AIX system, complete the following steps:

1. Ensure that the WebSphere Message Broker profile is in your shell profile, or source it manually by issuing the **`mqsiprofile`** command from the WebSphere Message Broker installation `bin` directory. For example:

   ```
   . /opt/ibm/mqsi/8.0.0.0/bin/mqsiprofile
   ```

2. If you want to disable `KK3UserExit` for a specific message flow, issue the following command:

   ```
   mqsichangeflowuserexits broker_name -e execution_group_name -f
   message_flow_name -a ""
   ```

3. Stop the WebSphere Message Broker instances on which you want to disable data collection using the `mqistop` *`broker_name`* command. For example:

   ```
   mqistop MB8BROKER
   ```

4. If you skipped step 2 and you want to disable `KK3UserExit` for all message flows on the WebSphere Message Broker instance, use the following command:

   ```
   mqsichangebroker broker_name -e
   ```

   For example:

   ```
   mqsichangebroker MB8BROKER -e ""
   ```

   Use this command to change the current state of the user exit to inactive for all message flows on the WebSphere Message Broker instance. To disable all user exits on the WebSphere Message Broker instance, issue the following command:

   ```
   mqsichangebroker broker_name -e ""
   ```

5. Navigate to the *`MB_DC_home`*`/bin` directory.
6. If you disabled `KK3UserExit` for all message flows, remove the `KK3UserExit` user exit library for the WebSphere Message Broker installation by issuing the following command:

   ```
   ./configDC.sh -disable broker_installation_directory
   ```

   For example, on AIX systems:

   ```
   /opt/IBM/ITM/aix513/k3/bin ./configDC.sh -disable /opt/IBM/mqsi/8.0.0.0
   ```

   For example, on Linux systems:

   ```
   /opt/IBM/ITM/ls3263/k3/bin ./configDC.sh -edisable /opt/IBM/mqsi/8.0.0.0
   ```

7. Restart the WebSphere Message Broker instances using the `mqistart` *`broker_name`* command. For example:

   ```
   mqistart MB8BROKER
   ```

Data collection is disabled for the specified message flows on the WebSphere Message Broker.

Before you uninstall ITCAM for SOA, you must disable data collection by removing `KK3UserExit` from all message flows and WebSphere Message Broker instances. For more information about uninstalling ITCAM for SOA, see

"Uninstalling IBM Tivoli Composite Application Manager for SOA on Windows systems" on page 72 on Windows systems or on Linux or AIX systems.

Disabling data collection on message flows

If you enabled data collection for a message flow that you no longer want to monitor, be sure to disable data collection for the message flow before the WebSphere Message Broker is stopped when you uninstall the data collector. If you do not disable the message flow first, you cannot list the message flow using the **`mqsilist`** command.

If the problem occurs, use one of the following procedures to recover the message flow:

- Using the Toolkit, remove the message flow and then redeploy it.
- Restore the original data collector user exit code to the correct location by completing the following steps:
  1. Reinstall the Data Collector for WebSphere Message Broker.
  2. Run the Data Collector for WebSphere Message Broker `ConfigDC` utility to enable the data collector:
  3. Restart the WebSphere Message Broker.
  4. Use the **`mqsilist`** command to verify that the message flow exists.

After you recover the message flow, disable data collection using the Data Collector for WebSphere Message Broker `configDC` utility

Part 4. Configuring ITCAM for SOA-specific data collectors for runtime environments

After you run the installation program to install application support for the monitoring server, portal server, and desktop client, and after you install and configure the monitoring agent on the systems where services are to be monitored, you must enable the various supported runtime environments for data collection.

This part of the *IBM Tivoli Composite Application Manager for SOA Installation Guide* describes the procedures for enabling and disabling data collection using ITCAM for SOA-specific data collectors for the various runtime environments supported with this version.

Chapter 10. Overview

ITCAM for SOA provides the following two ways to enable or disable data collection for your runtime environments:

- The Data Collector Configuration utility, which you can run in graphical user interface mode, console mode, or with a silent response file.
- The `KD4configDC` command-line script.

The Data Collector Configuration utility and the `KD4configDC` command-line script can be used to configure data collection for all application server environments, apart from the WebSphere Application Server environment.

Important:

- A separate set of configuration tools and sample response files are provided to configure ITCAM Data Collector for WebSphere. For information about configuring data collection for a WebSphere Application Server runtime environment, see Chapter 7, "Configuring data collection: WebSphere Application Server," on page 257.
- A separate set of configuration tools is provided to configure Data Collector for WebSphere Message Broker. For information about configuring data collection for a WebSphere Message Broker runtime environment, see Chapter 9, "Configuring data collection: WebSphere Message Broker," on page 359.

Enabling or disabling data collection if your application server is currently running

You do not have to stop your application server before you run the Data Collector Configuration utility or the `KD4configDC` script. However, because the ITCAM for SOA data collectors are integrated into the applications or the application server, you must stop and restart the application server sometime after enabling or disabling your data collectors and before starting the monitoring agent, in order for the data collection configuration to take effect. You might prefer to restart the application server during off-shift hours. Refer to the specific chapters in this guide related to your runtime environment for details.

For the BEA WebLogic Server, the application server *must* be running before you run the Data Collector Configuration utility or the `KD4configDC` script. If you later add additional applications to your BEA WebLogic Server, you might need to enable or disable data collection again.

Enabling or disabling data collection if you are installing over an existing installation

You might need to stop the application server before you run the configuration utility or the `KD4configDC` script, otherwise the existing JAR file might be locked and unable to be updated.

Enabling or disabling data collection if you are upgrading an existing installation

You must disable data collection before upgrading the monitoring agent. Refer to the documentation provided with the existing product for information about disabling data collection. See Part 1, “Installing the product,” on page 1 for more information about upgrading your existing installation.

Before enabling or disabling data collection

Some runtime environments require you to complete a few manual configuration tasks before running the Data Collector Configuration utility or the `KD4configDC` script. Refer to the chapters for each supported runtime environment in this guide for details on any manual steps you must complete before enabling or disabling data collection.

Permissions needed to configure for data collection

In general, you must have permission to run scripts in the *ITCAM4SOA_Home*`/KD4/bin` directory and you must have permission to add a handler to the application server you intend to monitor. The details of these permissions vary greatly according to the application server environment in question. Refer to the specific chapters for each application server for those details.

Setting up user permissions for non-root users

It is important on Linux and UNIX operating systems that the user who installed the monitoring agent and the user who owns the application server environment are in the same group (for example, `itmusers`) if non-root users are used. See “Permissions for installing, upgrading, or updating the monitoring agent” on page 83 for more information about setting up permissions.

To run the Data Collector Configuration utility, permissions are needed to complete the following:

- Run a Java application (and to use the X Window System on UNIX operating systems)
- Read and run additional shell scripts in *ITCAM4SOA_Home*`/KD4/bin`.

Additional permissions might be needed depending on the type of application server runtime environment for which data collection is being configured:

Microsoft .NET

If you plan to configure data collection using the ITCAM for SOA .NET data collector, you must have permission to complete the following:

- Copy files from *ITCAM4SOA_Home*`/KD4/lib` to the .NET Global Assembly Cache.
- Locate and edit the machine.config file, which is found inside the .NET directory structure.

BEA WebLogic Server

To configure the data collector to monitor requester applications (both standalone and those hosted inside server applications), you must edit the application as described in Chapter 12, “Configuring data collection: BEA WebLogic Server,” on page 399. To perform these tasks, your user must have all the permissions that are normally associated with application development and deployment.

In addition, you must have the authority to perform the following tasks:

- Stop and restart the application server.

- Add the ITCAM for SOA JAR file to the class path for the server. You should edit the server startup scripts to reference the JAR file that is installed into *ITCAM4SOA_Home*/KD4/lib.
- Have read access to %BEA_HOME%/registry.xml.

For BEA WebLogic Server version 8:

- You must provide a user name and password with permission to connect to the t3 service on the application server.
- You must have JDNI and JMX authority to access the weblogic.management.adminhome mbean.
- You must have JMX permission to discover web applications using WebServiceComponentMBean instances. You must have permission to edit the webservices.xml files for each web application. In the case of an Axis-based application, you must have permission to edit server-config.wsdd and client-config.wsdd.

For BEA WebLogic Server version 9:

- You must provide a user name and password with permission to connect to the t3 service on the application server.
- You must have JDNI and JMX authority to access the weblogic.management.mbeanservers.domainruntime mbean.
- You must have JMX authority to manipulate Web applications using the DomainRuntimeService mbeans.
- You must have authority to use these MBeans to edit the deployment descriptors of applications discovered by them.
- You must have authority to add JAR files from *ITCAM4SOA_Home*/KD4/lib/ into an applications WEB-INF/lib directory.

JBoss Permissions needed:

- Copy files from *ITCAM4SOA_Home*/KD4/lib to *JBOSS_HOME*/server/server/lib
- Make backup copies of deployment descriptors in the deploy/jboss-ws4ee.sar/META-INF/ directory for each server instance.
- Edit axis-server-config.wsdd and axis-client-config.wsdd
- Create a temporary directory under java.io.tmpdir, and read and write files within that directory.

SAP NetWeaver

Permissions needed:

- Copy a jar from *ITCAM4SOA_Home*/KD4/lib to the WEB-INF/ directory tree for each application.
- Edit lports_1.xml, protocols.txt, and application-j2ee-engine.xml files as appropriate for your application.
- Certain categories of applications must have programmatic changes in order to support monitoring, as described in Chapter 15, "Configuring data collection: SAP NetWeaver," on page 417. For these cases, your user must have the authority that is normally associated with application development and deployment.

WebSphere Community Edition

Permissions needed:

- Edit *WASCE_HOME*/bin/setenv.bat/sh
- Create and delete files in *WASCE_HOME*/temp/KD4
- Create and edit a file that will contain a list of applications.

- Edit the plan file for each affected application, webservices.xml, web.xml, and ejb-jar.xml files, as needed.

DataPower

To configure the DataPower environment for data collection, you need file system access to create and edit files in *ITCAM4SOA_Home*/KD4/config. However, you must supply a username and password that has authority to subscribe to the WS-Management Endpoint feature on the DataPower appliance. See "Configuring a user account on the DataPower SOA appliance" on page 445 for more information on this procedure.

Running the Data Collector Configuration utility

ITCAM for SOA provides the Data Collector Configuration utility to simplify the enabling and disabling of data collection for many of the supported runtime environments. The utility runs in either a graphical user interface mode, in console mode, or in silent mode. Logging functions are also provided to help you troubleshoot problems.

You start the Data Collector Configuration utility by running the ConfigDC script, located in the *ITCAM4SOA_Home*/KD4/bin directory where IBM Tivoli Composite Application Manager for SOA is installed. See "The IBM Tivoli Composite Application Manager for SOA home directory" on page xvi for information on resolving the value of *ITCAM4SOA_Home*.

On supported Windows operating systems, open a command prompt window and run the ConfigDC script using the following general format:

```
ConfigDC [–console | –silent [dir_path/]silent_file]
[–debug [dir_path/]debug_file]
```

On supported AIX, Solaris, HP-UX, and Linux operating systems, including z/OS® UNIX System Services, run the ConfigDC script using the following general format:

```
./ConfigDC.sh [–console | –silent [dir_path/]silent_file]
[–debug [dir_path/]debug_file]
```

These command options are described further in "ConfigDC script options."

Important: You can use the ConfigDC utility in the *ITCAM4SOA_Home*/KD4/bin directory in GUI mode, console mode, and silent mode to configure data collection for Microsoft .NET version 3.5 or earlier. You cannot use the ConfigDC utility to configure data collection for Microsoft .NET framework version 4.0. Instead, install the ITCAM for Microsoft Applications .NET data collector and complete the procedure in "Using the ITCAM for Microsoft Applications .NET data collector" on page 396 to configure data collection.

ConfigDC script options

Running the ConfigDC script with no options starts the Data Collector Configuration utility in the default graphical user interface mode. This is an InstallShield-based wizard that prompts you through several on-screen pages for the necessary parameters to enable or disable data collection for your supported runtime environment. See "Running the Data Collector Configuration utility graphical user interface" on page 379 for more information.

You can specify the following options with the ConfigDC script:

–console

This option runs the Data Collector Configuration utility in the command prompt window, if you prefer to use that instead of the InstallShield graphical user interface , or if you have no graphic console available. This option cannot be specified together with the `–silent` option. See "Running the Data Collector Configuration utility in console mode" on page 381 for more information about running the configuration utility in console mode.

Examples:

```
ConfigDC -console
./ConfigDC.sh -console
```

–silent [*dir_path*/]*silent_file*

This option runs the Data Collector Configuration utility in silent mode. The *silent_file* file is a simple properties file that you create, containing the necessary parameters to enable or disable data collection for your supported runtime environment. If this file is not stored in the *ITCAM4SOA_Home*`\KD4\bin` directory (see "The IBM Tivoli Composite Application Manager for SOA home directory" on page xvi for information on determining the value of *ITCAM4SOA_Home*), specify the fully qualified directory path *dir_path*, where this file is located. This option cannot be specified together with the `–console` option. See "Running the Data Collector Configuration utility in silent mode" on page 382 for more information about running the configuration utility in silent mode.

Examples:

```
ConfigDC -silent configdc_silent.txt
ConfigDC -silent C:\silentFiles\configdc.silent
./ConfigDC.sh -silent configdc.properties
```

–debug [*dir_path*/]*debug_file*

This option can be specified alone, or after specifying either the`–console` or `–silent` options. The Data Collector Configuration utility is run in either graphical user interface mode, console mode, or silent mode, and log information is written to the *debug_file* file for later examination and diagnosis of problems. The debug log file is a plain text file that is stored in the `\KD4\bin` directory if the optional *dir_path* is not specified, and can be opened using your preferred text editor. If you do not specify a file name for *debug_file*, then the operation is not performed, and you are presented with the syntax of the command as a reminder.

Examples:

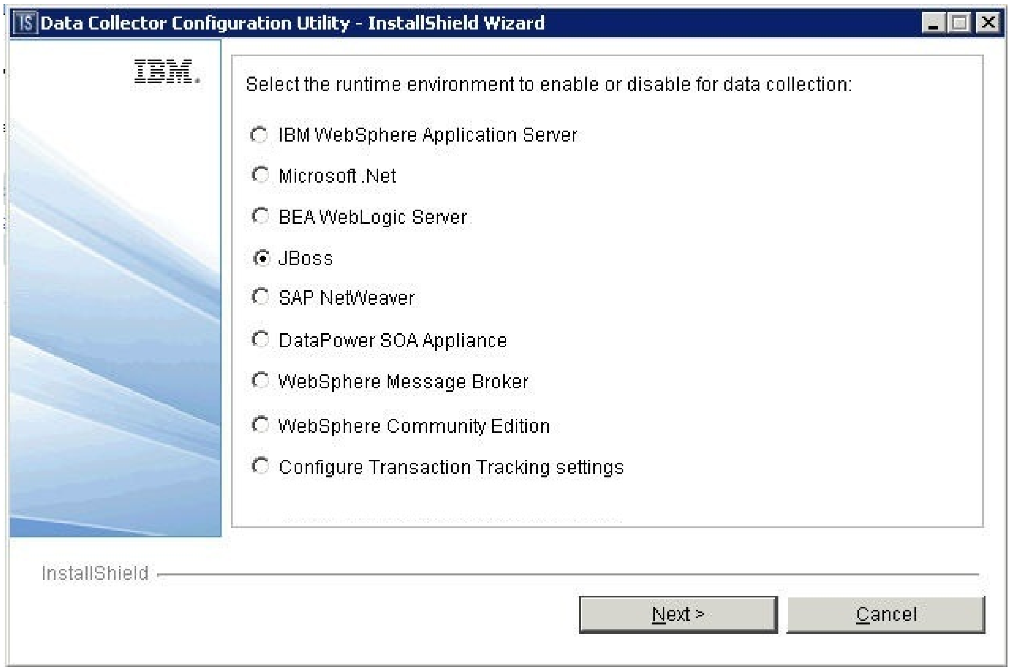
```
ConfigDC -debug configdc_log.txt
./ConfigDC.sh -console -debug debuglog
ConfigDC -silent C:\Properties\configdc.properties -debug configdc.log
```

Running the Data Collector Configuration utility graphical user interface

Running the ConfigDC script without specifying either the `–console` or `–silent` options starts the Data Collector Configuration utility using the default graphical user interface. Complete these steps:

1. You are prompted to select a language. Select an appropriate language and click **OK**.
2. The configuration utility is initialized and a welcome page with some brief information about the utility is presented. Click **Next**.
3. The Data Collector Configuration utility presents you with a selection menu of supported runtime environments for which you can enable or disable data

collection, as shown in Figure 53. Select a runtime environment and click **Next**.



Data Collector Configuration Utility - InstallShield Wizard

Select the runtime environment to enable or disable for data collection:

○ IBM WebSphere Application Server

○ Microsoft .Net

○ BEA WebLogic Server

● JBoss

○ SAP NetWeaver

○ DataPower SOA Appliance

○ WebSphere Message Broker

○ WebSphere Community Edition

○ Configure Transaction Tracking settings

Figure 53. Selecting a runtime environment to configure data collection

Depending on the runtime environment that you select, additional pages might be displayed where you are required to enter details specific to the runtime environments that you have selected. Refer to additional chapters in this guide (see “Configuring data collection for your environment” on page 394) for more details about the parameters that are needed to configure data collection for each supported runtime environment.

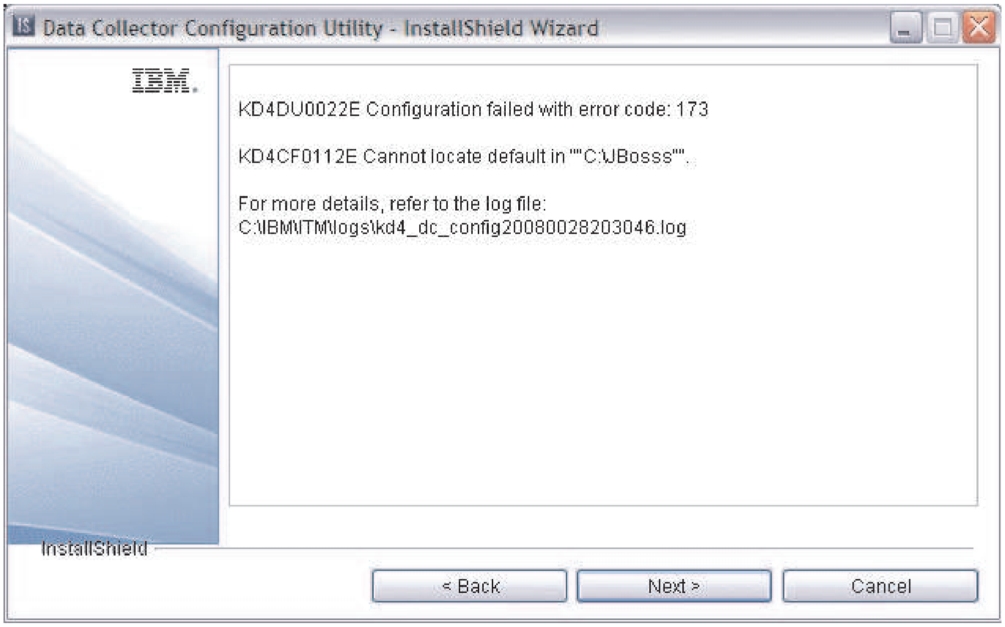
Remember:

- The Data Collector Configuration utility is no longer used to enable and disable data collection for a WebSphere Application Server or a WebSphere Message Broker runtime environment:
  - The **IBM WebSphere Application Server** option provides you with an option to open a console and start the ITCAM Data Collector for WebSphere Configuration utility for configuring data collection for a WebSphere Application Server. The ITCAM Data Collector for WebSphere Configuration utility can also be run directly from a command prompt.
  - To configure data collection for WebSphere Message Broker instances, use the `configDC` utility that is in the *MB_dc_home*`\bin` directory on Windows systems or in the *MB_dc_home*`/bin` directory on Linux and UNIX systems.

    The **WebSphere Message Broker** option is provided for disabling ITCAM for SOA version 7.2 WebSphere Message Broker data collector.
- You can use the Data Collector Configuration utility to configure data collection for JBoss version 4 application server environments. To configure data collection for JBoss version 5 environments, you must use the `KD4configDC` command.
- The Data Collector Configuration utility does not have an option to configure data collection for WebSphere Community Edition on Solaris platforms.

4. Follow the on-screen prompts, and wait for the completion of the configuration. An indication of successful or unsuccessful completion is displayed, and you are prompted to return to the main selection page to configure another runtime environment, or you can quit the Data Collector Configuration utility at any time.

If an error occurs during the configuration process, an appropriate error message is displayed, along with the directory path where the log file is located. You can then examine the log file for more information and take corrective action as needed. Figure 54 shows an example of how the configuration utility responds to an error caused during configuration of the JBoss runtime environment.



```
KD4DU0022E Configuration failed with error code: 173

KD4CF0112E Cannot locate default in ""C:\JBosss"".

For more details, refer to the log file:
C:\IBM\ITM\logs\kd4_dc_config20080028203046.log
```

Figure 54. An example of an error message displayed during configuration

Running the Data Collector Configuration utility in console mode

Running the ConfigDC utility with the `–console` option starts the Data Collector Configuration utility in the command window, if you prefer to use that option instead of the default graphical user interface.

You are prompted to select a language to use in the configuration utility, and a welcome response is displayed in the command window. You are prompted to continue by typing a numerical response. Be sure to choose a language for which your command window includes the necessary code page. See the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for additional information.

Throughout the use of the utility in console mode, you must respond by typing one of several valid responses. The wizard presents the same basic selection options as described in "Running the Data Collector Configuration utility graphical user interface" on page 379.

Changing the character set code page

In some situations, you might find that some characters on the Data Collector Configuration utility pages are not displayed correctly, possibly substituted with a question mark (?) or other unexpected characters. This might occur if, for example, you are running on a Windows operating system in Japanese and you choose to run the Data Collector Configuration utility in German.

To resolve this problem in console mode, you can change the Microsoft Windows character set code page for the current command prompt, using the **CHCP** command before running the Data Collector Configuration utility:

- For Italian, French, Spanish, and German languages, run this command:
  ```
  chcp 1252
  ```
- For Brazilian Portuguese, run this command:
  ```
  chcp 850
  ```

After running the CHCP command, run the Data Collector Configuration utility again in console mode and select the desired language. If the problem persists, you might need to change the font that is displayed by the console.

Important: The workaround is only required if you are running the `ConfigDMS` utility or the Data Collector Configuration utility in console mode and some characters are not displayed correctly.

Running the Data Collector Configuration utility in silent mode

Running the `ConfigDC` script with the `–silent` *`silent_file`* option starts the Data Collector Configuration utility in silent mode. Silent mode uses properties that are defined in the *silent_file* response file instead of interacting with you in the graphical user interface or in console mode. You cannot specify both `–silent` mode and `–console` mode together.

When you run the Data Collector Configuration utility in silent mode, the configuration parameters are read from a simple text response file, *silent_file*, that you create in advance. A typical response file might look similar to the following example:

```
# Sample silent configuration file
# File version - make sure that you are using proper version of silent file.
version=7.20.01.00

# To select configuration settings of Data Collector you want to enable/disable,
uncomment the corresponding line


# ------------------------------------------------------------------------------
######################   .Net section   ######################################
### Action

# DotNET.action=enable
# DotNET.action=disable
```

When you create a silent response file, keep these considerations in mind:

- A sample silent mode response file, `sample_silent.cfg`, is provided with the Data Collector Configuration utility in the *`ITCAM4SOA_Home`*`/KD4/bin` directory (see “The IBM Tivoli Composite Application Manager for SOA home directory” on page xvi for information about determining the value of *ITCAM4SOA_Home*).

  Tip: All lines are commented out using the # character. Be sure to remove the comment markings for each property that you plan to use, and save your changes to a unique file name.

- A line in the file starting with the # character is treated as a comment, and is not processed. If the # character is used elsewhere in the line, it is not considered to be the start of a comment. This means that you can use the # character in passwords or for other uses.
- The response file is coded using the ISO 8859-1 character set. If you specify any characters not in this character set, they must be represented with Unicode escapes.
- The properties file can include only one `version` property. This property might be useful for future releases if the format of the response file changes.
- Each property is described on a separate line, in the following format:

  `*data collector*.*property*.[*instance*]=*value*`

  data collector
  This is the name of the data collector for the given runtime environment, such as `*DataPower*` or `JBoss`, and others. The list of valid properties that you can configure is described in "Silent mode properties."

  property
  This is the name of property. The list of available properties is unique for every data collector. The `action` property is available for all data collectors, and can be one of two possible values, `enable` or `disable`. The list of valid properties that you can configure is described in "Silent mode properties."

  instance
  This is an optional designation for some data collectors, such as DataPower, that might monitor a set of application servers and DataPower appliances. For every such instance, use a unique value for *instance*.

  Using this additional qualifier, you can create multiple sections of your response file for a single data collector type. For example, you might create two DataPower sections in the response file, each section containing a group of uniquely defined DataPower properties. The first group of properties is specified with an *instance* value of `1`, and the second group with an instance value of `2`. See the descriptions in the sections that follow for data collector types that support multiple instances.

  value This is the value of the property. Property values can be blank, or empty. Note that an empty value results in the property not specified, as opposed to using a default value. To use the default value (if any), do not specify the property in the response file (or include it in a comment line).
- If a data collector is not specified in the silent response file, its parameters are not changed.
- Passwords are in plain text. When the configuration utility stores the password, it is hidden from view at that time for security.
- Properties and their values are case-sensitive.
- You can use a single silent response file to enable and disable multiple data collectors (for example, BEA and DataPower)

Silent mode properties

This section describes each group of property values that you can specify in the silent response file. The sample response file, `sample_silent_cfg`, also contains descriptive comments to help you understand when to use each property.

Note: Make sure to use the ITCAM for SOA 7.2 Fix Pack 1 version of the file.

Version: The *version* property is placed at the top of the response file and represents the version of the response file format. By default, this property is set to a value of `7.20.01.00`:

```
version=7.20.01.00
```

Microsoft .NET: The Microsoft .NET data collector type has this available property:

```
DotNET.action={enable | disable}
```

The `DotNET.action` property specifies whether to enable or disable data collection in the Microsoft .NET runtime environment. This is equivalent to the `–enable` and `–disable` options specified with the `KD4configDC` script. Examples (specify *either* of these properties, but not both):

```
DotNET.action=enable
DotNET.action=disable
```

Properties for Microsoft .NET do not have multiple instances, meaning you can only define one group of .NET properties in the response file, and the *instance number* format is not used.

BEA WebLogic Server: The BEA WebLogic Server data collector type has the following available properties:

```
BEA.action={enable | disable}
BEA.modified_env_file={true | false}
BEA.axis={true | false}
BEA.url=WebLogic_Server_URL
BEA.user_id=user_ID
BEA.user_password=password
```

The `BEA.action` property specifies whether to enable or disable data collection in the BEA WebLogic Server runtime environment installed at *WebLogic_Server_URL*. This is equivalent to the `–enable` and `–disable` options specified with the `KD4configDC` script. Examples (specify *either* of these properties, but not both):

```
BEA.action=enable
BEA.action=disable
```

The `BEA.modified_env_file` property confirms that you have modified the BEA application server classpath and prepended the `kd4dcagent.jar` file to the WEBLOGIC_CLASSPATH environment variable. For details on this manual modification, see step 2 on page 400. Examples (specify *either* of these properties, but not both):

```
BEA.modified_env_file=true
BEA.modified_env_file=false
```

The `BEA.axis` property specifies whether to configure data collection for the Apache Axis Web Services Engine, an optional feature of the BEA WebLogic Server. To configure the Apache Axis version, set this property to `true`, otherwise set it to `false`. If you do not specify this property, `false` is assumed as the default value. Examples (specify *either* of these properties, but not both):

```
BEA.axis=true
BEA.axis=false
```

The BEA.url property specifies the Web address (URL) of the BEA WebLogic Server, for example, t3://localhost:7001 (t3 and t3s are proprietary BEA protocols). This is equivalent to the *URL* option specified with the KD4configDC script. Example:

```
BEA.url=t3://localhost:7001
```

The BEA.user_id property specifies a valid BEA WebLogic Server user name with authority to configure applications. This is equivalent to the *userID* option specified with the KD4configDC script. Example:

```
BEA.user_id=user01
```

The BEA.user_password property specifies a valid password associated with the value specified for the BEA WebLogic Server user name, BEA.user_id. This is equivalent to the *password* option specified with the KD4configDC script. Example:

```
BEA.user_password=password
```

Refer to your BEA WebLogic documentation for more information on passwords for your authorized user names.

Properties for BEA WebLogic Server do not have multiple instances, meaning you can only define one group of BEA WebLogic Server properties in the response file, and the *instance number* format is not used.

JBoss: The JBoss Application Server data collector type has these available properties:

```
JBoss.action={enable | disable}
JBoss.configuration={default | all}
JBoss.home=JBoss_Home_Dir
```

The JBoss.action property specifies whether to enable or disable data collection on the JBoss application server that is installed at *JBoss_Home_Dir*. This is equivalent to the –enable and –disable options that are specified with the KD4configDC script. Examples (specify *either* of these properties, but not both):

```
JBoss.action=enable
JBoss.action=disable
```

The JBoss.configuration property specifies the type of JBoss application server to configure. These are the valid values:

default
This configuration type contains everything that is needed to run a standalone Java EE server.

all This configuration type starts all available services, including the RMI/IIOP and clustering services, and the Web services deployer, which are not loaded in the default configuration.

A third configuration type, minimal, is not supported, because this configuration does not include support for web services. Examples (specify *either* of these properties, but not both):

```
JBoss.configuration=default
JBoss.configuration=all
```

You can create a custom configuration with a unique name, if preferred.

The JBoss.home property specifies the base installation directory path for the JBoss application server, such as C:\JBoss. Examples:

```
JBoss.home=C:\\JBoss
JBoss.home="C:\\Program Files\\JBoss"
```

Tip:

1. The directory path backslash (\) character must be doubled (\\).
2. If the directory path contains a blank space, such as `C:\Program Files\JBoss`, the path must be enclosed in double quotation marks.

Properties for JBoss Application Server do not have multiple instances, meaning you can only define one group of JBoss properties in the response file, and the *instance number* format is not used.

SAP NetWeaver: The SAP NetWeaver data collector type has these available properties:

```
SAP.action.instance={enable | disable}
SAP.component.instance={1 | 2 | 3}
SAP.sapappsdir.instance=apps_dir
SAP.sid_home.instance=SAP_Home
SAP.sid.instance=sid_ID
```

Properties for SAP NetWeaver can have multiple instances, meaning you can define more than one group of SAP NetWeaver properties in the response file, using the additional *instance* qualifier in the property name. Example:

```
# SAP NetWeaver Instance 1
# All server applications under SID: j2e
SAP.action.1=enable
SAP.component.1=3
# SAP.sapappsdir.instance=apps_dir
SAP.sid_home.1=C:\\usr\\sap
SAP.sid.1=j2e
#
# SAP NetWeaver Instance 2
# Client side standalone Web services application
SAP.action.2=enable
SAP.component.2=2
SAP.sapappsdir.2=//opt//IBM//appsdir
# SAP.sid_home.instance=SAP_Home
# SAP.sid.instance=sid_ID
```

In the example, notice that each group is defined with its own unique instance number, and only those properties that are required by the specified type are defined. The unused properties remain commented out.

The `SAP.action.`*instance* property specifies whether to enable or disable data collection in the SAP NetWeaver runtime environment. This is equivalent to the `–enable` and `–disable` options specified with the `KD4configDC` script.

Examples (specify *either* of these properties, but not both):

```
SAP.action.1=enable
SAP.action.1=disable
```

The `SAP.component.`*instance* property specifies the type of SAP NetWeaver application to configure. These are the valid integer values:

1 Specify this value for a server side web services application if your server side application is not located under the a common SAP system ID (SID). This is equivalent to specifying the `–sapappsdir` option with the `KD4configDC` script. When you specify this type, you must also define the `SAP.sapappsdir.`*instance* property.

2 Specify this value for a client side standalone web services application. This is equivalent to specifying the `–clientappsdir` option with the KD4configDC script. When you specify this type, you must also define the `SAP.sapappsdir.`*instance* property.

3 Specify this value to configure all server-side web services applications under a specific SAP system ID (SID). This is equivalent to specifying the `–sid` option with the `KD4configDC` script. When you specify this type, you must also define the `SAP.sid_home.`*instance* and the `SAP.sid.`*instance* properties.

Tip: Use option 3 whenever possible. Option 3 provides some additional error checking of the directory structure for the SAP system ID that you specify, and avoids having to search the entire system for applications to configure.

The `SAP.sapappsdir.`*instance* property specifies the directory path for the services application being monitored. You must include this property in your response file if the `SAP.component.`*instance* property is defined with a value of 1 or 2. For a standalone client side application JAR file, specify the fully qualified directory path to the file. Examples:

```
SAP.sapappsdir.1=C:\\SAP_Apps\\
SAP.sapappsdir.1=/usr/sap_apps/Customer/EnterpriseSTDClientProxy.jar
```

Tip:

1. The directory path backslash (\) character must be doubled (\\).
2. If the directory path contains a blank space, such as `C:\Program Files\SAP_apps`, the path must be enclosed in double quotation marks.

The `SAP.sid_home.`*instance* property specifies the SAP home directory, typically `/usr/sap` or `C:\usr\sap`, though the directory can be located anywhere on your system. You must include this property in your response file if the `SAP.component.`*instance* property is defined with a value of 3. This is equivalent to specifying the *home* parameter for the `–sid` option when running the `KD4configDC` script. Examples:

```
SAP.sid_home=/usr/sap
SAP.sid_home=C:\\usr\\sap
```

Tip:

1. The directory path backslash (\) character must be doubled (\\).
2. If the directory path contains a blank space, such as `C:\Program Files\usr\sap`, the path must be enclosed in double quotation marks.

The `SAP.sid.`*instance* property specifies a common SAP system ID (SID). If you have multiple server-side web services applications under a common SID, you can configure all of them for data collection at the same time, by specifying the SID. This is equivalent to specifying the *sid* parameter for the `–sid` option when running the `KD4configDC` script. Example:

```
SAP.sid.1=j2e
```

DataPower: The DataPower data collector type has these available properties:

```
DataPower.action.<instance>={enable | disable}
DataPower.host.<instance>=<hostname>
DataPower.user_id.<instance>=<user_ID>
DataPower.user_password.<instance>=<password>
DataPower.port.<instance>=<port>
DataPower.poll.<instance>=<polling_interval>
DataPower.path.<instance>=<DP_SOA_appliance_path>
DataPower.domainlist.<instance>=<domain1>,<domain2>,...<domainN>
DataPower.displaygroup.<instance>=<display_group_name>
DataPower.maxrecords.<instance>=<max_records>
DataPower.subExpire.<instance>=<length_of_time_subscription_is_valid>
```

Properties for DataPower can have multiple instances, meaning you can define more than one group of DataPower properties in the response file, using the additional *<instance>* qualifier in the property name. Example:

```
# DataPower Instance 1
DataPower.action.1=enable
DataPower.host.1=dpbox1
DataPower.user_id.1=admin
DataPower.user_password.1=xxa1b2c3
# DataPower.port.1=5550
DataPower.poll.1=60
# DataPower.path.1=/
DataPower.domainlist.1=default1
DataPower.displaygroup.1=dpbox_disp1
# DataPower.subExpire.1=15
# DataPower.maxrecords.1=1000
#
# DataPower Instance 2
DataPower.action.2=enable
DataPower.host.2=dpbox2
DataPower.user_id.2=user12
DataPower.user_password.2=q1w2e3r4
# DataPower.port.2=5550
# DataPower.poll.2=10
# DataPower.path.2=/
DataPower.domainlist.2="userdom1,userdom2,userdom3"
DataPower.displaygroup.2=all_doms
# DataPower.subExpire.2=15
# DataPower.maxrecords.2=1000
```

In the example, notice that each group is defined with its own unique instance number, and only those properties that are required by the specified type are defined. The unused properties are commented out.

The data collector uses the values in the **DataPower.host.***<instance>*, **DataPower.port.***<instance>*, and **DataPower.path.***<instance>* properties to construct the Web address that is used as the target for messages sent to the DataPower SOA appliance. The Web address is constructed in this format:

```
https://<host>:<port>/<path>
```

The **DataPower.action.***<instance>* property specifies whether to enable or disable data collection in the DataPower runtime environment. This is equivalent to specifying the **–enable** and **–disable** options with the `KD4configDC` script.

Examples (specify ***either*** of these properties, but not both):

```
DataPower.action.1=enable
DataPower.action.1=disable
```

The **DataPower.host.***<instance>* property defines the DataPower SOA appliance host name or IP address. This host name is used to establish a socket connection, and is used as part of the Web address that points to the DataPower SOA appliance. This can be any length string, with no blank characters. This is equivalent to specifying the *<host>* parameter for the **–host** option when running the `KD4configDC` script. Example:

```
DataPower.host.1=dpbox1
```

See “Creating node names in Tivoli Enterprise Portal” on page 465 regarding possible truncation of this value in the node name. See “Considerations for enabling data collection for DataPower monitoring” on page 468 for more information about using this property.

The **DataPower.user_id.**<*instance*> property defines the DataPower SOA appliance authenticated user name. This user must be a valid user for the DataPower SOA appliance defined by the Host parameter. This is equivalent to specifying the <*user ID*> parameter for the **–user** option when running the `KD4configDC` script. Example:

```
DataPower.user_id.1=admin123
```

The **DataPower.user_password.**<*instance*> property defines the DataPower SOA appliance authentication password, entered in clear text (not encoded). This password must be valid for the user specified in the **DataPower.user_id.**<*instance*> property. This is equivalent to specifying the <*password*> parameter for the **–password** option when running the KD4configDC script. Example:

```
DataPower.user_password.1=xx123abc
```

The **DataPower.port.**<*instance*> property is an optional property that defines the DataPower SOA appliance port number. This port number is used to establish a socket connection and is used as part of the Web address pointing to the DataPower SOA appliance. The value specified must be an integer from 0 to 65535. If this parameter is not specified, the default value of *5550* is used. This is equivalent to specifying the <*port number*> parameter for the **–port** option when running the `KD4configDC` script. Example:

```
DataPower.port.1=5550
```

The **DataPower.poll.**<*instance*> property is an optional property that defines the DataPower SOA appliance polling interval, in seconds. The data collector waits this amount of time between each poll of the DataPower SOA appliance. The value of this property must be an integer from 1 to 300 (1 seconds to 5 minutes). If this parameter is not specified, the default value of *10* is used. This is equivalent to specifying the <*polling interval*> parameter for the **–poll** option when running the `KD4configDC` script. Example:

```
DataPower.poll.1=60
```

The **DataPower.maxrecords.**<*instance*> property is an optional property that defines the maximum number of records that the DataPower data collector can process from the DataPower SOA appliance per polling interval. The value of this property must be an integer value, between 1 and 30000. If this parameter is not specified, the default value of *15000* is used. This is equivalent to specifying the *maximum number of records* parameter for the **–maxrecords** option when running the `KD4configDC` script. Example:

```
DataPower.maxrecords.1=1000
```

Restriction: Setting this property in the silent configuration file is ineffective.

The **DataPower.subExpire.**<*instance*> property is an optional property that defines the length of time, in minutes, that the subscription of the DataPower data collector to the DataPower appliance remains valid. At the end of the subscription period, the DataPower data collector renews its subscription to the DataPower appliance. If this parameter is not specified, the default value of 15 is used. This must be an integer value, specified in minutes, between 3 and 30. Example:

```
DataPower.subExpire.1=15
```

Restriction: Setting this property in the silent configuration file is ineffective.

The **DataPower.path.**<*instance*> property is used as part of the Web address pointing to the DataPower SOA appliance. Its value is set to / by default. Example:

```
DataPower.path.1=/
```

Restriction: You cannot specify a path other than /. Changing the value of the property has no effect.

The **DataPower.domainlist.**<*instance*> property is an optional property that defines the list of domains to be monitored on the DataPower SOA appliance. The value for this property is specified in the form of a comma-separated list of domain names. Any domains in this list that are not authorized to the user defined by the **DataPower.user_id.**<*instance*> property are not monitored. Specify each domain name as any string, with no blank characters. If you specify more than one domain name, the entire list of comma-separated names must be enclosed in double quotation marks. This is equivalent to specifying the list of domain names for the **–domainlist** option when running the `KD4configDC` script. Examples:

```
DataPower.domainlist.1=domain1
DataPower.domainlist.1="domain1,domain2,domain3"
```

See "Considerations for enabling data collection for DataPower monitoring" on page 468 for more information about using this property.

The **DataPower.displaygroup.**<*instance*> property is an optional property that defines the DataPower SOA appliance display name. The name can be any string, with no blank characters, up to 64 characters long. This is equivalent to specifying the <*display group*> parameter for the **–displaygroup** option when running the `KD4configDC` script. Example:

```
DataPower.path.1=/
```

See "Creating node names in Tivoli Enterprise Portal" on page 465 regarding possible truncation of this value in the node name. See "Considerations for enabling data collection for DataPower monitoring" on page 468 for more information about using this property.

DataPower as a service: A special silent mode response file property is available for you to register the DataPower data collector as a Windows service or UNIX daemon:

```
DataPowerService.action={enable | disable}
```

This is equivalent to specifying the `–registerService` or `–deregisterService` options with the `KD4configDC` script. Examples (specify *either* of these properties, but not both):

```
DataPowerService.action=enable
DataPowerService.action=disable
```

Properties for registering DataPower as a service or daemon do not have multiple instances, meaning you can only define one group of properties in the response file, and the *instance number* format is not used.

WebSphere Message Broker: The WebSphere Message Broker data collector type has these available properties:

```
MessageBroker.action.instance={enable}
MessageBroker.allow_to_stop_mb.instance={true | false}
MessageBroker.broker_name.instance=broker
MessageBroker.execution_group_name.instance=group
MessageBroker.message_flow_name.instance=flow
```

Remember: The configDC utility can be used to disable an ITCAM for SOA version 7.2 WebSphere Message Broker data collector. The utility cannot be used to configure the Data Collector for WebSphere Message Broker. For information about configuring the data collection in ITCAM for SOA version 7.2 Fix Pack 1 or later, see Chapter 9, “Configuring data collection: WebSphere Message Broker,” on page 359.

Properties for WebSphere Message Broker can have multiple instances, meaning you can define more than one group of WebSphere Message Broker properties in the response file, using the additional *instance* qualifier in the property name. Example:

```
# WebSphere Message Broker Instance 1
MessageBroker.action.1=disable
MessageBroker.allow_to_stop_mb.1=true
MessageBroker.broker_name.1=testbroker
MessageBroker.execution_group_name.1=testGroup
MessageBroker.message_flow_name.1=testFlow
#
# WebSphere Message Broker Instance 2
MessageBroker.action.2=disable
MessageBroker.allow_to_stop_mb.2=true
MessageBroker.broker_name.2=WM_Broker
MessageBroker.execution_group_name.2=WMGroup1
MessageBroker.message_flow_name.2=WMFlow
```

In the example, notice that each group is defined with its own unique instance number, and that all properties are required.

The MessageBroker.action.*instance* property disables data collection in the WebSphere Message Broker runtime environment. This is equivalent to specifying the –disable option with the KD4configDC script. For example:

```
MessageBroker.action=disable
```

The MessageBroker.allow_to_stop_mb.*instance* property confirms that the message broker can be automatically stopped while data collection is configured, and then restarted after configuration is complete. Examples (specify *either* of these properties, but not both):

```
MessageBroker.allow_to_stop_mb.1=true
MessageBroker.allow_to_stop_mb.1=false
```

The MessageBroker.broker_name.*instance* property specifies the name of the message broker to be configured. This is equivalent to specifying the *broker_name* parameter with the KD4configDC script. Example:

```
MessageBroker.broker_name.1=BrokerName
```

The MessageBroker.execution_group_name.*instance* property specifies the name of the execution group in the specified WebSphere Message Broker to be configured. This is equivalent to specifying the *execution_group_name* parameter with the KD4configDC script. Example:

```
MessageBroker.execution_group_name.1=MB1_exgroup1
```

The MessageBroker.message_flow_name.*instance* property specifies the name of the message flow within the specified execution group to be configured. This is equivalent to specifying the *message_flow_name* parameter with the KD4configDC script. Example:

```
MessageBroker.message_flow_name.1=messageFlow1
```

Transaction Tracking Settings: In the sample response file, sample_silent_cfg, the following properties are available for configuring the transaction tracking settings:

```
TTAPI.action={enable | disable}
TTAPI.server.address=tcp:transaction_collector_IP_address:5455
```

The TTAPI.action property specifies whether to enable the sending of transaction tracking API events to a specified Transaction Collector. This is equivalent to the –enable and –disable options that are specified with the KD4configDC script. Examples (specify *either* of these properties, but not both):

```
TTAPI.action=enable
TTAPI.action=disable
```

The TTAPI.server property specifies the IP address of the Transaction Collector. This is equivalent to the –server option specified with the KD4configDC script:

```
TTAPI.server=tcp:collector.ibm.com:5455
```

Silent mode errors and messages

The Data Collector Configuration utility validates the operations and their values in the silent response file and displays a message when required values are missing or when a property is assigned to a value that is not valid.

The Data Collector Configuration utility displays messages describing the operations that are being performed by the utility and results of those operations (success or failure). Properties and their values in the silent response property file are validated by the utility. When an error occurs, the error code and the error message are displayed describing the cause of the failure, if possible.

If the silent response file contains configuration properties for several data collectors, and errors occur while attempting to configure one of the data collectors, the utility attempts to continue to configure the remaining data collectors specified in the file.

If you attempt to configure multiple instances of a data collector that does not support multiple instances, error messages are displayed and the configuration of all instances of that data collector are ignored. The utility attempts to configure other data collectors specified in the silent response property file.

Additional configuration options

In addition to enabling or disabling data collection for supported runtime environments, the Data Collector Configuration utility also registers or deregisters DataPower as a system service or UNIX daemon.

Running the KD4configDC script

As an alternative to using the Data Collector Configuration utility to enable or disable data collection for supported runtime environments, you can use the KD4configDC script, located in the *ITCAM4SOA_Home*/KD4/bin directory where IBM Tivoli Composite Application Manager for SOA is installed. See “The IBM Tivoli

Composite Application Manager for SOA home directory" on page xvi for information about how to determine the value of *ITCAM4SOA_Home*.

On supported Windows operating systems, run the KD4configDC script using the following general format:

```
KD4configDC {–enable | –disable} –env x environment specific arguments
```

On supported AIX, Solaris, HP-UX, and Linux operating systems, including z/OS UNIX System Services, run the KD4configDC script using the following general format:

```
./KD4configDC.sh {-enable | -disable} -env x environment specific arguments
```

Important:

- Starting with ITCAM for SOA version 7.2, it is no longer possible to configure data collection for the WebSphere Application Server using the KD4configDC script. For more information about configuring data collection for WebSphere Application Server environments, see Chapter 7, "Configuring data collection: WebSphere Application Server," on page 257.
- Starting with ITCAM for SOA version 7.2 Fix Pack 1, it is no longer possible to configure data collection for WebSphere Message Broker using the KD4configDC script. For information about configuring data collection for a Websphere Message Broker environments, see Chapter 9, "Configuring data collection: WebSphere Message Broker," on page 359.

  Remember: You can use the KD4configDC script to unconfigure an ITCAM for SOA version 7.2 WebSphere Message Broker data collector.
- You can use the KD4configDC script to configure data collection for Microsoft .NET version 3.5 or earlier. The KD4configDC must not be used to configure data collection for Microsoft .NET framework version 4.0. Instead, install the ITCAM for Microsoft Applications .NET data collector and complete the procedure in "Using the ITCAM for Microsoft Applications .NET data collector" on page 396 to configure data collection.

The following parameters and values are defined for these commands:

–enable
Specify this required parameter to enable the specified runtime environment for data collection. You must specify either the–enable or –disable parameter, but not both.

–disable
Specify this required parameter to disable the specified runtime environment for data collection. You must specify either the –enable or –disable parameter, but not both.

–env x Specify this required parameter to identify the type of runtime environment to be enabled or disabled for data collection. The value of x is an integer from 2 to 4, 6 to 8, or the integer 10, indicating one of the following supported runtime environments:

- 2 = Microsoft .NET
- 3 = BEA WebLogic Server
- 4 = JBoss Application Server
- 6 = SAP NetWeaver
- 7 = WebSphere Community Edition
- 8 = DataPower

environment specific arguments

This parameter is actually one or more parameters unique to each type of supported runtime environment. Depending on the value specified for `x` in the `–env x` parameter, the parameters that are specified with the `KD4configDC` script vary. These runtime environment-specific arguments are further detailed in the sections that follow, along with more detailed information about each supported runtime environment.

Getting help for KD4configDC

You can type the following command to view the online help for the `KD4configDC` script:

```
KD4configDC -h
```

For Linux, AIX, HP-UX, or Solaris operating systems, type the following command to view the online help for the KD4configDC script:

```
./KD4configDC.sh -h
```

Messages related to running the `KD4configDC` script are documented in the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*.

Configuring data collection for your environment

Refer to the following sections for more information about each supported runtime environment and the specific parameters and values needed to enable and disable data collection in each environment. If you have problems with the Data Collector Configuration utility or in running the `KD4configDC` script, refer to the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for more information.

- Chapter 11, “Configuring data collection: Microsoft .NET,” on page 395
- Chapter 12, “Configuring data collection: BEA WebLogic Server,” on page 399
- Chapter 13, “Configuring data collection: JBoss,” on page 409
- Chapter 14, “Configuring data collection: CICS Transaction Server,” on page 415
- Chapter 15, “Configuring data collection: SAP NetWeaver,” on page 417
- Chapter 16, “Configuring data collection: WebSphere Community Edition,” on page 431
- Chapter 17, “Configuring data collection: DataPower SOA Appliance,” on page 441
- Chapter 18, “Integrating with ITCAM for Transactions,” on page 489

Chapter 11. Configuring data collection: Microsoft .NET

ITCAM for SOA provides support for monitoring web services that run in a Microsoft .NET application server runtime environment. The list of versions of Microsoft .NET supported by ITCAM for SOA 7.2 Fix Pack 1 and later is available from the Software product compatibility reports website. For information about accessing reports from this website, see “Required software” on page 15.

ITCAM for Microsoft Applications provides a data collector, .NET Data Collector version 7.3.1, for monitoring transactions that occur in a .NET framework application. You can use the ITCAM for Microsoft Applications data collector for tracking web services for ITCAM for SOA. ITCAM for Microsoft Applications version 6.3 is provided with ITCAM for Applications version 7.2.

After you install and configure the ITCAM for Microsoft Applications .NET data collector, you integrate the data collector with ITCAM for SOA. The data collector sends web services data to the ITCAM for SOA agent. The data is displayed in the ITCAM for SOA workspaces in the Tivoli Enterprise Portal.

ITCAM for SOA provides its own .NET data collector for monitoring web services that occur in a .NET framework. You can use the ITCAM for SOA data collector for tracing web services for ITCAM for SOA. After you install and configure ITCAM for SOA, you enable data collection using the data collector configuration utilities. The ITCAM for SOA data collector sends web services data to the ITCAM for SOA agent. The data is displayed in the ITCAM for SOA workspaces in the Tivoli Enterprise Portal.

Your decision to configure data collection for Microsoft .NET using the ITCAM for SOA or the ITCAM for Microsoft Applications data collector depends on the version of .NET you plan to monitor:

- To monitor web services in Microsoft .NET version 4.0, you must use ITCAM for Microsoft Applications .NET Data Collector version 7.3.1.
- To monitor web services in Microsoft .NET version 3.5 or earlier, either use ITCAM for Microsoft Applications .NET Data Collector version 7.3.1 for data collection or the ITCAM for SOA version 7.2 Fix Pack 1 or later .NET data collector.

To configure the .NET Data Collector version 7.3.1, use the utilities that are provided with ITCAM for Microsoft Applications. To configure the ITCAM for SOA .NET data collector, use the utilities that are provided with ITCAM for SOA.

Both the ITCAM for SOA and the ITCAM for Microsoft Applications data collectors can be integrated with ITCAM for Transactions. If configured, transaction events are sent to a Transaction Collector, which stores and aggregates transaction data from multiple data collectors. For more information about configuring the interface to ITCAM for Transactions, see Chapter 18, “Integrating with ITCAM for Transactions,” on page 489.

ITCAM for Transactions provides its own .NET data collector. When you install the .NET data collector as part of an ITCAM for Transactions installation, you replace the ITCAM for SOA .NET data collector. When you configure data collection, you enable data collection for ITCAM for SOA. For the installation and configuration steps, see the ITCAM for Transactions information center.

Important: if any of the following products are installed on the same system, use only one of them to collect data for ITCAM for SOA for .NET environments. You must not enable data collection for ITCAM for SOA from more than one of the products:

- ITCAM for Transactions
- ITCAM for Microsoft Applications
- ITCAM for SOA component in ITCAM for Applications

Using the ITCAM for Microsoft Applications .NET data collector

You can use the ITCAM for Microsoft Applications data collector for tracking web services for ITCAM for SOA.

Remember: The ITCAM for Microsoft Applications .NET data collector must be used to monitor Microsoft .NET version 4.0 and later.

To configure data collection using the ITCAM for Microsoft Applications .NET data collector, complete the following steps:

1. Install and start the ITCAM for SOA agent version 7.2 Fix Pack 1 (see Chapter 2, "Installing or upgrading ITCAM for SOA on Windows systems," on page 35).

   Remember: Do not configure the ITCAM for SOA .NET data collector. Selecting .NET option of the ITCAM for SOA `ConfigDC` utility adds older versions of the Tivoli libraries to the .NET environment.
2. Install ITCAM for Microsoft Applications .NET Data Collector version 7.3.1. For information about installing the data collector, the "Installing .NET Data Collector" in the ITCAM for Microsoft Applications information center.
3. (Optional) Configure the ITCAM for Microsoft Applications .NET data collector to monitor .NET transactions. For information about integrating the data collector with ITCAM for Microsoft Applications, see "Configuring .NET Data Collector" in the ITCAM for Microsoft Applications information center.
4. Integrate the ITCAM for Microsoft Applications .NET data collector with the ITCAM for SOA agent.
   a. Navigate to the `ITM\TMAITM6\K4\config` directory and modify the `dotNetDcConfig.properties.inactive` file as follows:
      ```
      default.kd4.enabled=true
      ```
   b. Navigate to the `ITM\TMAITM6\K4\bin` directory.
   c. Issue the **`configdc activateconfig`** command to activate the configuration change.
   d. Issue the **`iisreset`** command from a command prompt window to reset the IIS Server.
   e. If you have not already integrated the .NET or DataPower data collector with ITCAM for Transactions, issue the **`configdc registerdc`** command to register the .NET data collector as an administrator.
   f. Restart the ITCAM for SOA monitoring agent for the change to take effect.
5. (Optional) Integrate the ITCAM for Microsoft Applications .NET data collector with ITCAM for Transactions. For information about configuring the transaction tracking API for Microsoft .NET, see Chapter 18, "Integrating with

ITCAM for Transactions," on page 489. Microsoft .NET transaction data is displayed in the ITCAM for Transactions workspaces in the Tivoli Enterprise Portal. This step is not required if you issued the **configdc registerdc** command to register the .NET Data Collector.

For information about installing and configuring .NET Data Collector version 7.3.1, see *IBM Tivoli Composite Application Manager for Microsoft Applications: .NET Data Collector User's Guide* in the ITCAM for Microsoft Applications information center.

Using the ITCAM for SOA .NET data collector

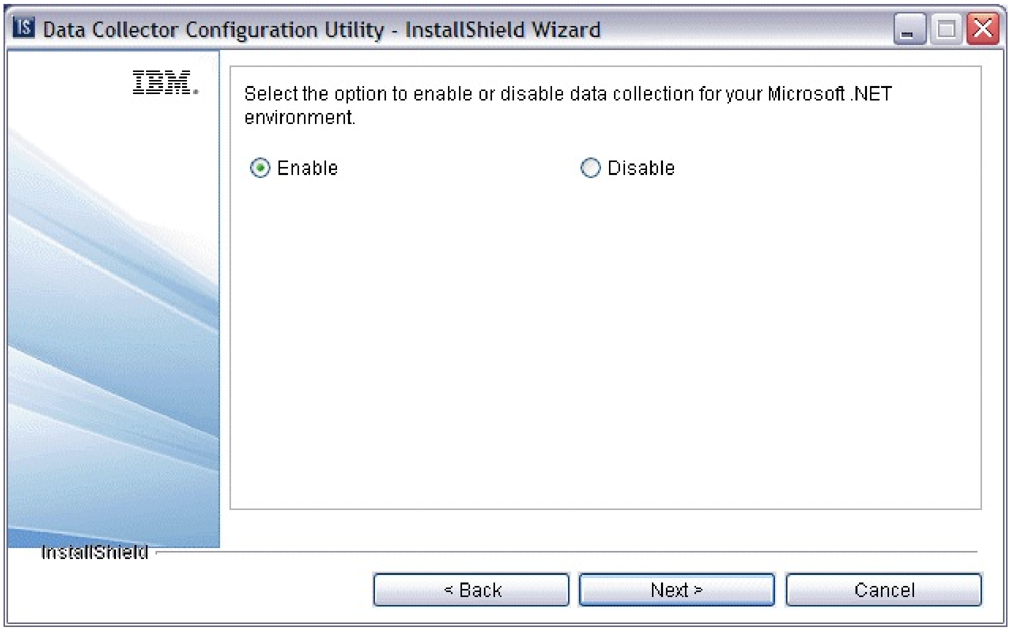
If you plan to monitor Microsoft .NET version 3.5 or earlier and you have not installed ITCAM for Microsoft Applications version 6.2, you can use the ITCAM for SOA .NET data collector to monitor web services.

To enable or disable data collection for the ITCAM for SOA .NET data collector, use the Data Collector Configuration utility that is provided with ITCAM for SOA.

Enabling data collection

Enable data collection using either the Data Collector Configuration utility or by running the **KD4configDC** command.

- To enable data collection using the Data Collector Configuration utility, complete these steps:



Data Collector Configuration Utility - InstallShield Wizard

Select the option to enable or disable data collection for your Microsoft .NET environment.

● Enable ○ Disable

Figure 55. Enabling data collection on Microsoft .NET

1. Start the Data Collector Configuration utility in either the default graphical user interface mode, in console mode, or in silent mode. See "Running the Data Collector Configuration utility" on page 378 for more information.
2. Select the option to configure Microsoft .Net.
3. Select the option to enable data collection.
4. Wait for the configuration utility to complete the operation.
5. Exit the utility.

- To enable data collection using the **KD4configDC** command, run the following command from a command prompt window (see "Running the KD4configDC script" on page 392 for more information):

  ```
  KD4configDC –enable –env 2
  ```

  For this command, no additional application server runtime environment-specific parameters are required.

Multiple messages

The configuration process attempts to configure data collection for all instances of the Microsoft .NET framework that it finds on the computer. This might result in certain messages being repeated, once for each Microsoft .NET instance found.

Tip: You do not have to restart the Microsoft .Net server after enabling the environment for data collection.

Disabling data collection

To disable data collection in the Microsoft .Net, environment, run either the Data Collector Configuration utility or the `KD4configDC` command.

- To disable data collection using the Data Collector Configuration utility, complete these steps:
  1. Run the Data Collector Configuration utility in either the default graphical user interface mode, in console mode, or in silent mode. See "Running the Data Collector Configuration utility" on page 378 for more information.
  2. Select the option to configure Microsoft .Net.
  3. Select the option to disable data collection.
  4. Wait for the configuration utility to complete the operation.
  5. Exit the utility.
- To disable data collection using the **KD4configDC** command, run the following command from a command prompt window (see "Running the KD4configDC script" on page 392 for more information):

  ```
  KD4configDC –disable –env 2
  ```

Multiple messages

The configuration process attempts to configure data collection for all instances of the Microsoft .NET framework that it finds on the computer. This might result in certain messages being repeated, once for each Microsoft .NET instance found.

You do not have to restart the Microsoft .Net server after disabling the environment for data collection.

Chapter 12. Configuring data collection: BEA WebLogic Server

This chapter describes the ITCAM for SOA data collector support for the BEA WebLogic Server runtime environments. Support is also provided for the Apache Axis SOAP engine running in the BEA WebLogic application server runtime environment. You can optionally choose to enable this Apache Axis support if needed.

The list of versions of BEA WebLogic Server and Apache Axis SOAP engine supported by ITCAM for SOA 7.2 is available from the Software product compatibility reports website. For information about accessing reports from this website, see "Required software" on page 15.

In the BEA WebLogic Server environment, the process of configuring for data collection adds the JAX-RPC handler to the `web-services.xml` deployment descriptor for each deployed service running on a local BEA application server. Before you can enable this environment for data collection, you must perform a few additional steps to prepare for both client-side and server-side configuration.

About Apache Axis

Apache Axis is a SOAP engine, defined on the official Apache Axis web site (http://ws.apache.org/axis/java/install.html) as "a framework for constructing SOAP processors such as clients, servers, gateways, etc". Axis runs as several servlets, while the BEA WebLogic application server provides the Web container for these Axis servlets. Conceptually, consider this environment as a BEA WebLogic server with Axis service support.

When Axis is installed according to the basic Axis installation instructions (see the Apache Axis web site for more information about basic and advanced installation options), Axis is deployed as a Web application to the Web container in either an exploded directory or a packaged war file, for example `axis.war`.

You deploy your services into this Axis web application by adding new classes and registering the new service into the Axis web application. The Axis data collector, when enabled for the Axis web application, monitors these services. If you deploy additional services after the Axis data collector is enabled for data collection, the newly deployed services are monitored automatically.

Message logging and message rejection are supported in the same manner as the BEA WebLogic Server data collector.

BEA client side configuration

Because BEA client applications that use the Web Services stack do not have deployment descriptors, you must add the ITCAM for SOA handler programmatically using the `javax.xml.rpc.handler.HandlerInfo` and `javax.xml.rpc.handler.HandlerRegistry` classes. The following example is sample client application for BEA WebLogic Server version 8:

```
import java.util.ArrayList;
import java.io.IOException;
import javax.xml.namespace.QName;
import javax.xml.rpc.ServiceException;
import javax.xml.rpc.handler.HandlerInfo;
import javax.xml.rpc.handler.HandlerRegistry;

public class Main{
  public static void main( String[] args ){
    . . .
  }
  public Main( String wsdl ){
    try {

      someService service = new someService_Impl( wsdl );
      someServicePort port = service.getSomeServicePort();
      . . .
      QName listQname[] = new QName[1];
      listQname[0] = new QName("http://www.ibm.com/KD4","ITCAM_for_SOA");

      List handlerList = new ArrayList();
      handlerList.add( new
        HandlerInfo( com.ibm.management.soa.agent.bea.ITMBEAClientHandler.class,
        null, listQname) );
      HandlerRegistry registry = service.getHandlerRegistry();
      registry.setHandlerChain( portName, handlerList );

       port.someWSCall();

    } catch( IOException e ) {
       . . .
    } catch( ServiceException e ) {
       . . .
    }
  }
}
```

BEA Version 9 class name

For BEA WebLogic Server version 9, the sample application is the same as for version 8, except that the class name should be `com.ibm.management.soa.agent.bea9.ITMBEAClientHandler.class`.

For more information , see your BEA WebLogic Server product documentation.

BEA server side configuration

Before you enable data collection, complete the following steps:

1. Shut down the BEA Server, following the instructions in the product documentation. You can use the Administration Console or the BEA WebLogic Administrative utility.
2. Modify the BEA application server classpath. To modify the classpath for *all domains*, edit the **commEnv.cmd** (or, for UNIX operating systems, **commEnv.sh**) script file in *WebLogic_HOME*/common/bin and append the kd4dcagent.jar file to the WEBLOGIC_CLASSPATH environment variable. For example:
   - On Windows operating systems, edit the **commEnv.cmd** script:

     ```
     set WEBLOGIC_CLASSPATH=
       %JAVA_HOME%\lib\tools.jar;...;C:\IBM\ITM\tmaitm6\KD4\lib\kd4dcagent.jar
     ```

   - On AIX operating systems, edit the **commEnv.sh** script:

```
WEBLOGIC_CLASSPATH=
  "${JAVA_HOME}/lib/tools.jar...
   ${CLASSPATHSEP}/candle/aix513/d4/KD4/lib/kd4dcagent.jar"
export WEBLOGIC_CLASSPATH
```

- On Solaris operating systems, edit the **commEnv.sh** script:

```
WEBLOGIC_CLASSPATH=
  "${JAVA_HOME}/lib/tools.jar...
   ${CLASSPATHSEP}/candle/sol283/d4/KD4/lib/kd4dcagent.jar"
export WEBLOGIC_CLASSPATH
```

To modify the Classpath for a *specific* BEA WebLogic Server domain, edit the **setDomainEnv.cmd** or **setDomainEnv.sh** script, in the `\bin` directory for the domain, and prepend the `kd4dcagent.jar` file onto the `PRE_CLASSPATH` environment variable.

3. Start the BEA WebLogic Server, following the instructions in the product documentation. You can use the Administration Console or the BEA WebLogic Administrative utility.

Enabling data collection in a single server environment

After you complete the previous steps to prepare for client-side and server-side installation, enable the environment for data collection using either the Data Collector Configuration utility or by running the `KD4configDC` command. Before enabling data collection, do these initial steps as needed:

1. On supported HP-UX operating systems, switch to the Korn shell (/usr/bin/ksh) interactive command interpreter.
2. Run a script to set up all the environment variables and Java options before enabling the environment for data collection.
   - For Windows operating systems:

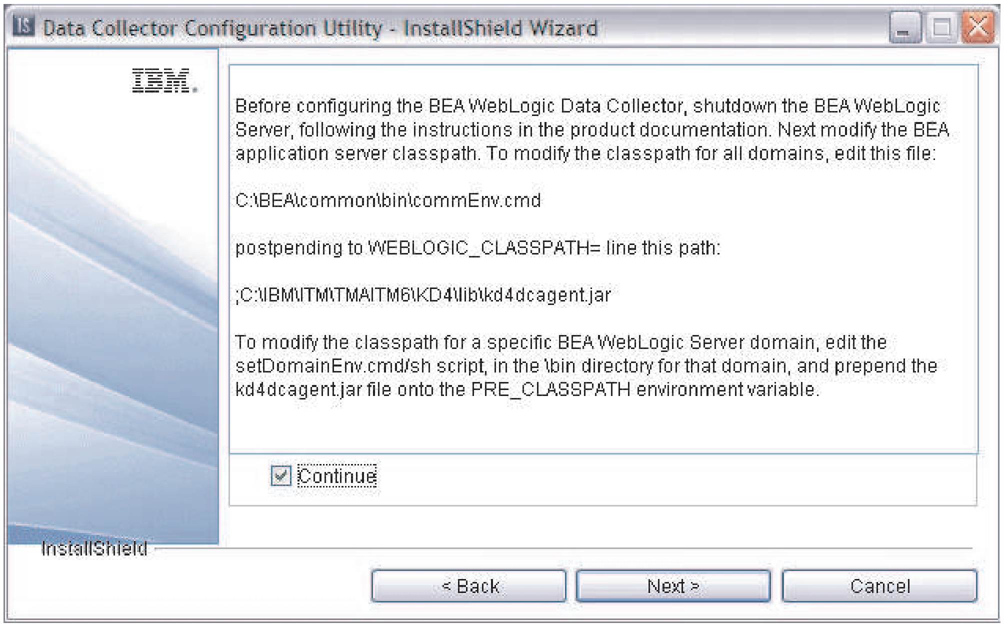
     DOMAIN_HOME\setDomainEnv.cmd (or setEnv.cmd)
   - For Linux, AIX, HP-UX, or Solaris operating systems:

     . /*DOMAIN_HOME*/setDomainEnv.sh (or setEnv.sh)

Using the Data Collector Configuration utility

Using the Data Collector Configuration utility, complete these steps:

1. Start the Data Collector Configuration utility in either the default graphical user interface mode, in console mode, or in silent mode. See "Running the Data Collector Configuration utility" on page 378 for more information.
2. Select the option to configure BEA WebLogic Server.
3. If the *BEA_HOME* system variable is not set, you are instructed to exit the configuration utility, run the `setEnv` script, and then run the utility again.
4. You are prompted to confirm that you have modified either the common environment (`commEnv.cmd` or `commEnv.sh`) or the domain-specific environment (`setDomainEnv.cmd` or `setDomainEnv.sh`) script to include the `kd4dcagent.jar` in the class path, and that the BEA WebLogic server should have been restarted. Confirm that these steps have been completed, and proceed with configuration.


Before configuring the BEA WebLogic Data Collector, shutdown the BEA WebLogic Server, following the instructions in the product documentation. Next modify the BEA application server classpath. To modify the classpath for all domains, edit this file:

C:\BEA\common\bin\commEnv.cmd

postpending to WEBLOGIC_CLASSPATH= line this path:

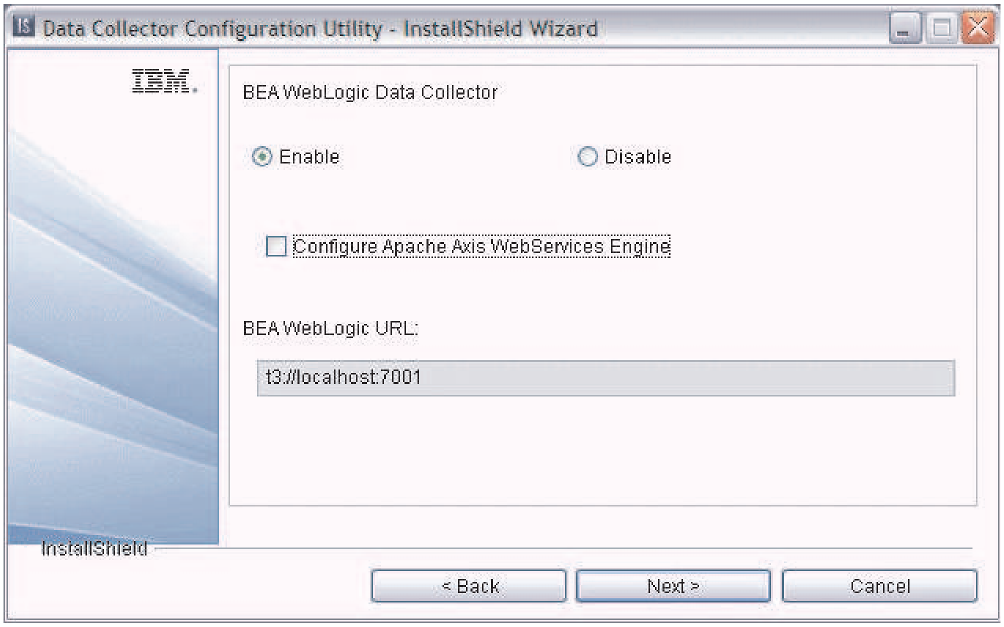
;C:\IBM\ITM\TMAITM6\KD4\lib\kd4dcagent.jar

To modify the classpath for a specific BEA WebLogic Server domain, edit the setDomainEnv.cmd/sh script, in the \bin directory for that domain, and prepend the kd4dcagent.jar file onto the PRE_CLASSPATH environment variable.

☑ Continue

Figure 56. Confirm that you have included `kd4dcagent.jar` in BEA application server classpath.

5. Select the option to enable data collection.
6. If you are using the optional Apache Axis support for the BEA WebLogic environment, select the check box **Configure Apache Axis WebServices Engine**. Otherwise verify that this check box is cleared.
7. Specify the Web address of the BEA WebLogic Server (for example, `t3://localhost:7001`, where `t3` and `t3s` are proprietary BEA protocols).


BEA WebLogic Data Collector

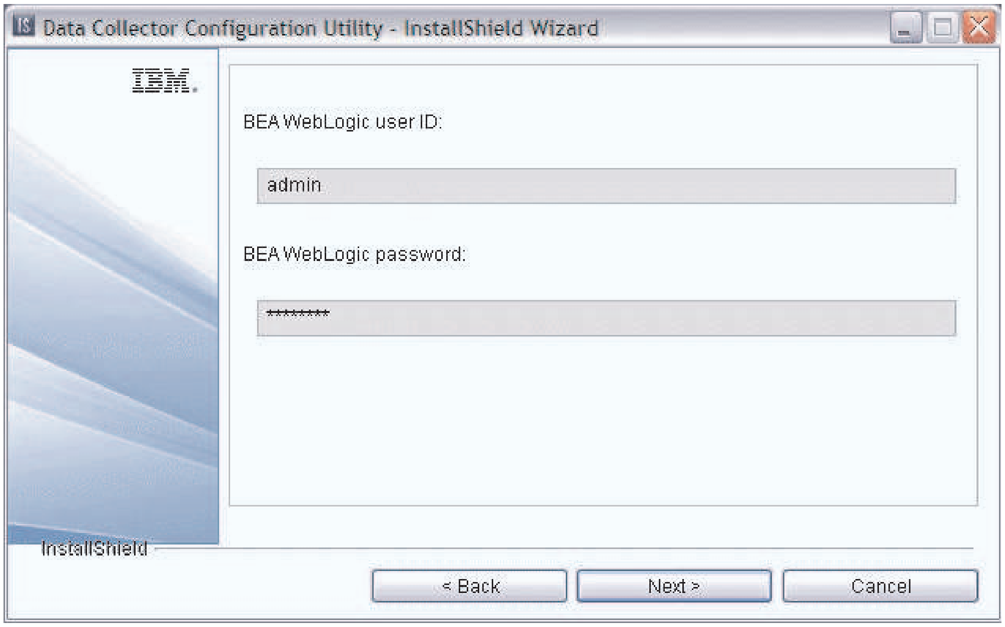
● Enable ○ Disable

□ Configure Apache Axis WebServices Engine

BEA WebLogic URL: t3://localhost:7001

Figure 57. Select the enable option and specify the URL for the BEA WebLogic server.

8. Specify the BEA WebLogic user name and password with the authority to configure applications.



BEA WebLogic user ID:

admin

BEA WebLogic password:

****

Figure 58. Specifying the BEA WebLogic user name and password

9. Wait for the configuration utility to complete the operation.
10. Repeat these steps as needed to enable data collection for other Web services implementations.
11. Exit the utility.

Restart the BEA WebLogic Server

After enabling data collection on your BEA WebLogic Server, stop and restart the server to complete the configuration.

Using the KD4configDC command

Using the **KD4configDC** command, run the following command from a command prompt window (see "Running the KD4configDC script" on page 392 for more information):

```
KD4configDC -enable -env 3 URL userID password [-axis]
```

In this command, these options and parameters are passed:

URL The Web address of the BEA WebLogic Server (for example, t3://localhost:7001). t3 and t3s are proprietary BEA protocols.

userID A valid WebLogic user name with the authority to configure applications.

password
A valid password associated with the specified WebLogic user name.

–axis This is an optional parameter that, when included in the command, enables the Apache Axis version of the data collector in the BEA WebLogic Server environment.

Examples:

```
KD4configDC -enable -env 3 "t3://localhost:7001"  weblogic weblogic
KD4configDC -enable -env 3 "t3://localhost:7001"  weblogic weblogic -axis
```

Restart the BEA WebLogic Server

After enabling data collection on your BEA WebLogic Server, stop and restart the server to complete the configuration.

Disabling data collection in a single server environment

To disable data collection in the BEA WebLogic Server environment, run either the Data Collector Configuration utility or the `KD4configDC` command. Before disabling data collection, do these initial steps as needed:

1. On supported HP-UX operating systems, switch to the Korn shell (/usr/bin/ksh) interactive command interpreter.
2. Run a script to set up all the environment variables and Java options before disabling the environment for data collection.
   - For Windows operating systems:

     `DOMAIN_HOME\setDomainEnv.cmd (or setEnv.cmd)`
   - For Linux, AIX, HP-UX, or Solaris operating systems:

     `. /DOMAIN_HOME/setDomainEnv.sh (or setEnv.sh)`

Using the Data Collector Configuration utility

Using the Data Collector Configuration utility, complete these steps:

1. Start the Data Collector Configuration utility in either the default graphical user interface mode, in console mode, or in silent mode. See “Running the Data Collector Configuration utility” on page 378 for more information.
2. Select the option to configure BEA WebLogic Server.
3. Select the option to disable data collection.
4. Specify the Web address of the BEA WebLogic Server (for example, `t3://localhost:7001`, where `t3` and `t3s` are proprietary BEA protocols).
5. If you are using the optional Apache Axis support for the BEA WebLogic environment, select the check box **Configure Apache Axis WebServices Engine**. Otherwise verify that this check box is cleared.
6. Specify the user name and password with the authority to configure applications.
7. Wait for the configuration utility to complete the operation.
8. Repeat these steps as needed to disable data collection for other Web service implementations.
9. Exit the utility.

Using the KD4configDC command

Using the `KD4configDC` command, run the following command from a command prompt window (see “Running the KD4configDC script” on page 392 for more information):

```
KD4configDC -disable -env 3 URL userID password [-axis]
```

In this command, these options and parameters are passed:

URL The Web address of the BEA WebLogic Server (for example, `t3://localhost:7001`). `t3` and `t3s` are proprietary BEA protocols.

userID A valid WebLogic user name with the authority to configure applications.

password
A valid password associated with the specified WebLogic user name.

–axis This is an optional parameter that, when included in the command, disables the Apache Axis version of the data collector in the BEA WebLogic Server environment.

Examples:

```
KD4configDC -disable -env 3 "t3://localhost:7001"  weblogic weblogic
KD4configDC -disable -env 3 "t3://localhost:7001"  weblogic weblogic -axis
```

Restart the BEA WebLogic Server

After disabling data collection on your BEA WebLogic Server, stop and restart the server to complete the configuration.

Enabling data collection in a BEA WebLogic multi-server environment

A typical BEA WebLogic domain contains one administrative server and one or more managed servers. To enable data collection in the domain, you need to enable data collection on only the administrative server, and then restart the managed servers for the configuration to take effect.

To enable data collection on BEA WebLogic servers in a domain, complete the following steps:

1. If you have not already done so, install the ITCAM for SOA monitoring agent on each BEA WebLogic managed and administrative server computer.
2. Modify the BEA application server classpath on all of the affected computer systems in the domain, using the procedure described in “BEA server side configuration” on page 400.
3. Before enabling the environment for data collection on supported HP-UX operating systems, switch to the Korn shell (/usr/bin/ksh) interactive command interpreter.
4. Run a script to set up all of the environment variables and Java options before enabling the environment for data collection.
   - For Windows operating systems:
     `DOMAIN_HOME\setDomainEnv.cmd (or setEnv.cmd)`
   - For Linux, AIX, or HP-UX, Solaris operating systems:
     `. /DOMAIN_HOME/setDomainEnv.sh (or setEnv.sh)`
5. Ensure that all of the servers in the cluster, including the administrative server, are running.
6. Enable the environment for data collection using either the Data Collector Configuration utility or by running the `KD4configDC` command.
   - Using the Data Collector Configuration utility, complete these steps:
     a. Start the Data Collector Configuration utility in either the default graphical user interface mode, in console mode, or in silent mode. See “Running the Data Collector Configuration utility” on page 378 for more information.
     b. Select the option to configure BEA WebLogic Server.
     c. If the *BEA_HOME* system variable is not set, you are instructed to exit the configuration utility, run the `setEnv` script, and then run the utility again.

d. You are prompted to confirm that you have modified either the common environment (**commEnv.cmd** or **commEnv.sh**) or domain-specific environment (**setDomainEnv.cmd** or **setDomainEnv.sh**) script to include the kd4dcagent.jar in the class path, and that the BEA WebLogic administrative server should have been restarted. Confirm that these steps have been completed, and proceed with configuration.

e. Select the option to enable data collection.

f. Specify the Web address of the BEA WebLogic administrative server (for example, t3://localhost:7001, where t3 and t3s are proprietary BEA protocols).

g. If you are using the optional Apache Axis support for the BEA WebLogic environment, select the **Configure Apache Axis WebServices Engine** check box. Otherwise verify that this check box is cleared.

h. Specify the user name and password with the authority to configure applications.

i. Wait for the configuration utility to complete the operation.

j. Exit the utility.

- Using KD4configDC, run the following command from a command prompt window (see "Running the KD4configDC script" on page 392 for more information):

```
KD4configDC.sh –enable –env 3 URL userID password [–axis]
```

URL The Web address of the BEA WebLogic Server (for example, t3://localhost:7001). t3 and t3s are proprietary BEA protocols.

userID A valid WebLogic user name with the authority to configure applications.

password
A valid password associated with the specified WebLogic user name.

–axis This is an optional parameter that, when included in the command, enables the Apache Axis version of the data collector in the BEA WebLogic Server environment.

Example:

```
KD4configDC -enable -env 3 "t3://localhost:7001"  weblogic weblogic
KD4configDC -enable -env 3 "t3://localhost:7001"  weblogic weblogic -axis
```

7. Restart the servers.

After enabling data collection, stop and restart all of the servers in the cluster, including the administrative server, to complete the configuration.

Disabling data collection in a BEA WebLogic multi-server environment

A typical BEA WebLogic domain contains one administrative server and one or more managed servers. To disable the AXIS data collector in the domain, you only need to disable the AXIS data collector on the administrative server and then restart the managed servers for the change to take effect.

This procedure assumes that the ITCAM for SOA monitoring agent is already installed on each BEA WebLogic server computer.

To disable the AXIS data collector on WebLogic servers in a domain, complete the following steps:

1. Before disabling the environment for data collection on supported HP-UX operating systems, switch to the Korn shell (/usr/bin/ksh) interactive command interpreter.
2. Run a script to set up all of the environment variables and Java options before disabling the environment for data collection.
   - For Windows operating systems:

     ```
     DOMAIN_HOME\setDomainEnv.cmd (or setEnv.cmd)
     ```
   - For Linux, AIX, or HP-UX, Solaris operating systems:

     ```
     . /DOMAIN_HOME/setDomainEnv.sh (or setEnv.sh)
     ```
3. Ensure that all of the servers in the cluster, including the administrative server, are running.
4. Run either the Data Collector Configuration utility or the `KD4configDC` command.
   - Using the Data Collector Configuration utility, complete these steps:
     a. Start the Data Collector Configuration utility in either the default graphical user interface mode, in console mode, or in silent mode. See "Running the Data Collector Configuration utility" on page 378 for more information.
     b. Select the option to configure BEA WebLogic Server.
     c. Select the option to disable data collection.
     d. Specify the Web address of the BEA WebLogic administrative server (for example, `t3://localhost:7001`, where `t3` and `t3s` are proprietary BEA protocols).
     e. If you are using the optional Apache Axis support for the BEA WebLogic environment, select the check box **Configure Apache Axis WebServices Engine**. Otherwise verify that this check box is cleared.
     f. Specify the user name and password with the authority to configure applications.
     g. Wait for the configuration utility to complete the operation.
     h. Exit the utility.
   - Using `KD4configDC`, run the following command from a command prompt window (see "Running the KD4configDC script" on page 392 for more information):

     ```
     KD4configDC -disable -env 3 URL userID password [-axis]
     ```

     URL The Web address of the BEA WebLogic administrative server (for example, `t3://localhost:7001`). `t3` and `t3s` are proprietary BEA protocols.

     userID A valid WebLogic user name with the authority to configure applications.

     password
     A valid password associated with the specified WebLogic user name.

     –axis This is an optional parameter that, when included in the command, disables the Apache Axis version of the data collector in the BEA WebLogic Server environment.

     Example:

     ```
     KD4configDC -disable -env 3 "t3://localhost:7001"  weblogic weblogic
     KD4configDC -disable -env 3 "t3://localhost:7001"  weblogic weblogic -axis
     ```
5. Restart the servers.

After disabling data collection, stop and restart all of the servers in the cluster, including the administrative server, to complete the configuration.

Apache Axis Limitations

The Apache Axis version of the data collector in the BEA WebLogic Server environment has these limitations:

- The Axis data collector supports monitoring services in Axis SOAP engines that are installed with *basic* installation (Web application) and *advanced* installation (adding Axis to an existing enterprise application) procedures. ITCAM for SOA does not support the enabling of monitoring for *customized* installations. See the Axis documentation for more details.
- The Axis data collector monitors both requester-side and provider-side service events, but only within supported application server runtime environments. Stand-alone client Axis applications are not supported.
- When monitoring both the Axis SOAP engine and the *native* SOAP engine of BEA WebLogic application servers, all services are displayed in the Tivoli Enterprise Portal as though they are running in the same runtime environment. There is no way to tell from the Tivoli Enterprise Portal which services are deployed to the Axis SOAP engine and which are deployed to the native SOAP engine.

Additional considerations

The port number attribute for the application server is always displayed with a value of `0` in the ITCAM for SOA attribute groups when running on BEA WebLogic version 9.2. If you have more than one server instance using the same name, and they are on the same computer, the data collected and processed for these instances is displayed as if they all came from a single server.

For information about monitoring and managing your services in a BEA WebLogic Server application server runtime environment, see the *IBM Tivoli Composite Application Manager for SOA User's Guide*.

Chapter 13. Configuring data collection: JBoss

This section describes the support for JAX-RPC services that are running on JBoss versions 4 and 5 Java Platform, Enterprise Edition (Java EE) and JAX-WS services running on JBoss version 5 Java EE.

The list of versions of JBoss supported by ITCAM for SOA 7.2 Fix Pack 1 is available from the Software product compatibility reports website. For information about accessing reports from this website, see "Required software" on page 15.

Enabling data collection

Enable data collection using either the Data Collector Configuration utility or by running the `KD4configDC` command. For JBoss version 5, you can enable data collection using the `KD4configDC` command only.

Important:

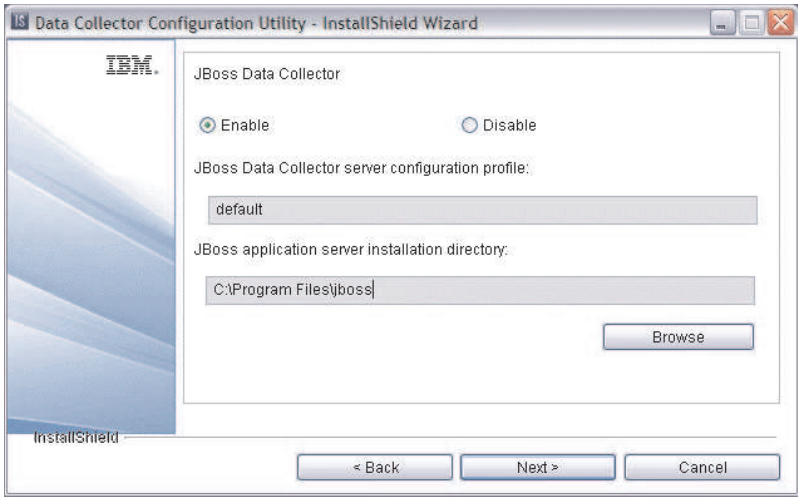
- You need to enable data collection only once in a JBoss version 4 application server runtime environment. When you add new applications to the environment, the data collector begins to monitor the new applications automatically.
- In a JBoss version 5 application server runtime environment, the data collector monitors an application automatically if the application does not have an annotation that overwrites the default handler chain (using `@HandlerChain`) or the endpoint configuration (using `@EndpointConfig`). However, if the application implements a custom handler or endpoint annotation, you must disable and then re-enable data collection using the `KD4configDC` command to monitor the application.

Enabling data collection for JBoss V4 environments using the Data Collector Configuration utility

To enable JBoss version 4 environments for data collection using the Data Collector Configuration utility, complete the following steps:

1. Optionally stop the JBoss application server before you enable the data collection.

   You do not have to stop the application server before you enable data collection. However, the data collector does not begin to collect data until after the JBoss application server is stopped and restarted. You might prefer to stop and restart the JBoss application server during off-peak hours. Refer to your JBoss documentation for the specific procedure to stop the JBoss application server.
2. Start the Data Collector Configuration utility in either the default graphical user interface mode, in console mode, or in silent mode. See "Running the Data Collector Configuration utility" on page 378 for more information.
3. Select the option to configure JBoss.
4. Select the option to enable data collection.



Data Collector Configuration Utility - InstallShield Wizard

JBoss Data Collector

● Enable ○ Disable

JBoss Data Collector server configuration profile:

default

JBoss application server installation directory:

C:\Program Files\jboss

Figure 59. Enabling data collection on JBoss

5. Specify the profile name in the field **JBoss Data Collector server configuration profile**. The profile `default` is chosen by default. Valid values are as follows:

   default
   The `default` configuration type contains everything that is needed to run a standalone Java EE server. The profile *default* is chosen by default.

   all The `all` configuration type starts all available services, including the RMI/IIOP and clustering services and the services deployer, which are not loaded in the *default* configuration.

   A third default configuration type, *minimal*, is not supported because this configuration does not include support for services.

   You can also create your own server configuration type by modifying the *default* or *all* types, or mixing and matching capabilities from either or both, and saving it as a new server configuration type name.
6. Specify the JBoss application server installation directory. For example, on Windows operating systems, `C:\Program Files\jboss`.
7. Wait for the configuration utility to complete the operation.
8. Exit the utility.
9. Restart the JBoss application server (refer to your JBoss documentation for the specific procedure). The data collector becomes active after the JBoss application server is restarted.

Enabling data collection using the `KD4ConfigDC` command

To enable data collection for a JBoss environment using the `KD4configDC` command, use the following syntax:

```
KD4configDC -enable -env 4 profile_name|profile_home
 JBoss_home [jmx_userID jmx_Password]
```

Where:

profile_name
The type of JBoss application server to be configured. The valid values are as follows:

default
The `default` configuration type contains everything that is needed to run a standalone Java EE server.

all The `all` configuration type starts all available services, including the RMI/IIOP and clustering services and the services deployer, which are not loaded in the *default* configuration.

A third default configuration type, *minimal*, is not supported, because this configuration does not include support for services.

You can also create your own server configuration type by modifying the *default* or *all* types, or mixing and matching capabilities from either or both, and saving it as a new server configuration type name. Then, you specify the name of the new server configuration profile in the `KD4configDC` command.

profile_home
The directory path name of the JBoss profile. You can specify a profile that is outside of the JBoss installation home directory. The *profile_home* variable can be specified when you configure data collection for a JBoss version 5 environment only.

JBoss_Home
The directory path name where the JBoss application server is installed, for example, `C:\JBoss` on a Windows operating system.

Tip: If the path name contains a blank space, you must ensure that the entire path is surrounded in quotation marks.

If you defined an environment variable for this directory path, *JBoss_Home* is an optional parameter.

jmx_userID
(Optional) The JBoss Management Console (JMX console) user name. If security is enabled for the JBoss environment, you must provide the JMX console user name and password. The *jmx_userID* variable can be specified when you configure data collection for a JBoss version 5 environment only.

jmx_password
(Optional) The JMX console password. The *jmx_password* variable can be specified when you configure data collection for a JBoss version 5 environment only.

To enable JBoss applications for data collection using the `KD4configDC` command, complete the following steps:

1. Optionally stop the JBoss application server before you enable the data collection.

   You do not have to stop the application server before enabling data collection, but the data collector does not begin to collect data until after the JBoss application server is stopped and restarted. You might prefer to stop and restart the JBoss application server during off-peak hours. Refer to your JBoss documentation for the specific procedure to stop the JBoss application server.
2. Enter the `KD4configDC` command from a command prompt window.

   For more information about starting the `KD4configDC` script, see "Running the KD4configDC script" on page 392.
3. Navigate to the `*ITCAM4SOA_Home*/KD4/bin` directory.

See "The IBM Tivoli Composite Application Manager for SOA home directory" on page xvi for information on resolving directory path variables.

4. Enable data collection for the JBoss application server environment using the `KD4ConfigDC` command. The following are some examples of enabling data collection:

   -
     ```
     KD4configDC.bat -enable -env 4 default
     ```

     Enable data collection on a supported Windows system. In this example, the default server configuration is used, and the *JBoss_Home* environment variable is used to specify the JBoss base installation directory. The command completes with a return code of 0.

   -
     ```
     ./KD4configDC.sh -enable -env 4 all /opt/jboss/jboss-eap-4.0/jboss-as
     ```

     Enable data collection on a supported UNIX and Linux operating systems. In this example, the `all` server configuration profile is specified to enable monitoring of a JBoss configuration where all services are started. The JBoss base installation directory is explicitly specified. Because there are no blank spaces in the path, the argument is specified without surrounding quotation marks.

   -
     ```
     KD4configDC.bat -enable -env 4 myConfig
     ```

     In this example, the user-defined server configuration profile `myConfig` is specified, and the *JBoss_Home* environment variable is used by default to specify the JBoss base installation directory.

   -
     ```
     KD4configDC.bat -enable -env 4 default "C:\App Servers\JBoss"
     ```

     In this example, the JBoss base installation directory is specified explicitly, and because there is a blank space in the path, the argument is surrounded by quotation marks.

   -
     ```
     KD4configDC.bat -enable -env 4 C:\apps_root\profile1 C:\jboss-soa-p-5\jboss-as
     ```

     In this example, data collection is configured for a JBoss version 5 application server environment. A profile home directory is specified. The profile home directory is outside of the JBoss base installation directory.

   -
     ```
     KD4configDC.bat -enable -env 4 C:\apps_root\profile1 C:\jboss-soa-p-5\jboss-as admin admin
     ```

     In this example, data collection is configured for a JBoss version 5 application server environment. The optional JMX console user name and password parameters are specified.
5. Restart the JBoss application server (refer to your JBoss documentation for the specific procedure). The data collector becomes active after the JBoss application server is restarted.

Important: When there are multiple server instances within the same JBoss application server runtime environment, you must run the `KD4configDC` command for each instance.

Disabling data collection

To disable data collection in a JBoss application server runtime environment, either use the Data Collector Configuration utility or run the `KD4configDC` command. For JBoss version 5, you can disable data collection using the `KD4configDC` command only.

Disabling data collection for JBoss V4 environments using the Data Collector Configuration utility

To disable data collection for JBoss version 4 environments using the Data Collector Configuration utility, complete these steps:

1. Start the Data Collector Configuration utility in either the default graphical user interface mode, in console mode, or in silent mode. See “Running the Data Collector Configuration utility” on page 378 for more information.
2. Select the option to configure JBoss.
3. Select the option to disable data collection.
4. Specify the profile name. The profile *default* is chosen by default. If you specify the profile name, you can change this to *all* or you can specify the name of a customized configuration profile that you created.
5. Specify the JBoss application server installation directory. For example, on Windows operating systems, `C:\Program Files\JBoss`.
6. Wait for the configuration utility to complete the operation.
7. Exit the utility.

Disabling data collection using the `KD4ConfigDC` command

Use the following syntax to disable data collection for a JBoss application server environment with the `KD4configDC` command:

```
KD4configDC -disable -env 4 profile_name|profile_home
 JBoss_Home [jmx_userID jmx_Password]
```

Where:

profile_name
: The type of JBoss application server to be configured. These are the valid values:

  default
  : The `default` configuration type contains everything that is needed to run a standalone Java EE server.

  all The `all` configuration type includes all available services.

  custom The name of a customized configuration profile that you created.

profile_home
: The directory path name of the JBoss profile. You can specify a profile that is outside of the JBoss installation home directory. The *profile_home* variable can be specified when you configure data collection for a JBoss version 5 or later environment only.

JBoss_home
: The directory path name where the JBoss application server is installed, for example, `C:\JBoss` on a Windows operating system.

  Tip: If the path name contains a blank space, you must ensure that the entire path is surrounded in quotation marks.

  If you defined an environment variable for this directory path, *JBoss_Home* is an optional parameter.

jmx_userID
: (Optional) The JMX console user name. If security is enabled for the JBoss environment, you must provide the JMX console user name and password.

The *jmx_userID* variable can be specified when you configure data collection for a JBoss version 5 or later environment only.

jmx_password

(Optional) The JMX console password. The *jmx_password* variable can be specified when you configure data collection for a JBoss version 5 or later environment only.

To disable data collection using the `KD4configDC` command, complete these steps:

1. Enter the `KD4configDC` command from a command prompt window.

   See "Running the KD4configDC script" on page 392 for more information.
2. Navigate to *`ITCAM4SOA_Home`*`/KD4/bin` directory location.

   See "The IBM Tivoli Composite Application Manager for SOA home directory" on page xvi for information about resolving directory path variables.
3. Using the `KD4configDC` command, disable data collection for the JBoss application server environment. For example:
   On supported Windows systems:

   ```
   KD4configDC.bat -disable -env 4 default C:\jboss4
   ```

   For example, on supported UNIX and Linux operating systems:

   ```
   ./KD4configDC.sh -disable -env 4 default /opt/jboss/jboss-eap-4.0/jboss-as
   ```
4. After the command completes, restart the JBoss application server.

   The JBoss data collector continues to collect data until the JBoss application server is restarted.

Important: When there are multiple server instances within the same JBoss application server runtime environment, you must run the `KD4configDC` command for each instance.

Additional considerations

As you enable and use data collection in the JBoss environment, keep in mind that if you attempt to enable or disable data collection multiple times in a row (for example, an enable followed by another enable), only the first invocation takes effect.

Chapter 14. Configuring data collection: CICS Transaction Server

IBM Customer Information Control System Transaction Server (CICS TS) running on the z/OS operating system acts as both an SOA server and client. The z/OS version of CICS TS features the following capabilities, which make it more feasible to implement CICS TS services using SOA in your production environment:

- Multiple message handlers per CICS region
- Multiple pipelines
- Use of either HTTP transport or WebSphere/MQ transport
- Support for simple object access protocol (SOAP) version 1.2
- New resources to ease configuration of services
- New APIs to manage SOA requests

The ITCAM for SOA CICS TS data collector monitors service flows to and from a CICS TS region, and provides the same services management and availability information that ITCAM for SOA currently provides for other application server runtime environments. Services data is presented in the Tivoli Enterprise Portal using the usual workspaces and views associated with IBM Tivoli Composite Application Manager for SOA.

Running within the CICS TS region, ITCAM for SOA acts as an SOA request monitor, intercepting incoming and outgoing SOA requests and rejecting incoming and outgoing messages according to user-configured filtering criteria. ITCAM for SOA stores message information, metrics and rejection information into log files for later processing. It also controls the amount of monitoring and message rejection that is performed. These functions are accomplished with minimal effect on the function being monitored as well as the overall performance of the CICS region.

Tip: Because message correlation is not supported in this data collector, services data collected in the CICS TS environment is not supported by the IBM Web Services Navigator tool.

Important:

- In ITCAM for SOA version 7.2 or later, the CICS TS data collector is not updated. To install the data collector, install and configure the data collector provided by ITCAM for SOA version 7.1.1 in your z/OS environment.
- If SOA Domain Management Server is deployed in your environment, the CICS TS data collector must integrate with an SOA Domain Management Server from ITCAM for SOA version 7.1.1. Otherwise, if you integrate the data collector with an SOA Domain Management Server from ITCAM for SOA version 7.2, CICS service data is not displayed in the topology workspaces in the Tivoli Enterprise Portal.

For more information about configuring the ITCAM for SOA CICS TS data collector in the z/OS environment, see the *Configuring IBM Tivoli Composite Application Manager for SOA on z/OS* guide.

Chapter 15. Configuring data collection: SAP NetWeaver

This section describes the support for the monitoring of services flows in the SAP NetWeaver environment.

The list of versions of SAP NetWeaver supported by ITCAM for SOA 7.2 Fix Pack 1 is available from the Software product compatibility reports website. For information about accessing reports from this website, see “Required software” on page 15.

Depending on the types of services applications you plan to monitor, you might need to enable or disable your SAP NetWeaver applications for the data collector using these different procedures:

- For a server-side application or for a stand-alone (running as a Java application) client application, you need to run only the Data Collector Configuration utility or the `KD4configDC` command to enable or disable the SAP NetWeaver application environment for data collection.
- For a deployable (running on a Java EE container) client application, you must manually modify the client code as described in the following sections.

Manually enabling applications with open source projects

The data collector for SAP NetWeaver includes third party software (also referred to as *excluded components*) as a part of monitoring services traffic in the SAP NetWeaver environment. See the license files in your appropriate language for more information on this third party software. These files are located in the *ITM_Home*`\license\D4V710` directory on the computer systems where the data collector support for Tivoli Monitoring is installed. See “The IBM Tivoli Composite Application Manager for SOA home directory” on page xvi for information about resolving directory path variables.

If any of the applications in your server use any of these excluded components, you must manually enable your applications as described in the sections that follow. As with any change, back up your application before making this change, and test it thoroughly afterward.

If this is not a concern for your installed applications, use the Data Collector Configuration utility or the **KD4configDC** command to enable all of the applications in your server. These methods, however, cannot enable services client calls made from within another service. These calls must be enabled manually as described in the sections that follow in order to be monitored.

You run the Data Collector Configuration utility or the `KD4configDC` command once to enable all SAP NetWeaver applications for data collection, and the data collector monitors all of the SAP NetWeaver related applications. If you add more SAP NetWeaver applications to the environment, you must run the Data Collector Configuration utility or the `KD4configDC` command again to enable these new applications for data collection. Applications that are already enabled are not affected.

Stand-alone client restriction

A supported SAP NetWeaver stand-alone client application must include an instance of the implementation for com.sap.engine.services.webservices.jaxrpc.wsdl2java.ServiceBase. To create an instance of java.rmi.Remote,javax.xml.rpc.Stub, the stand-alone client application must call getPort() or getLogicalPort() for the instance of com.sap.engine.services.webservices.jaxrpc.wsdl2java.ServiceBase.

Important: Do not use the `new` operator to create the instance of java.rmi.Remote,javax.xml.rpc.Stub.

User permission to write to log files

After enabling the data collector to monitor your SAP applications, ensure that the user ID that you use to start the SAP server has permission to write into the `\KD4\logs` directory.

Enabling data collection

There are several different patterns through which services components can operate on your SAP NetWeaver application server, and each is configured slightly differently. Use the following sections to identify the correct mechanisms for your applications, and choose whether to use the Data Collector Configuration utility or the `KD4configDC` command to enable or disable data collection, or whether you should do so manually:

- "All server applications under a SAP system ID"
- "A server application not located under a SAP system ID" on page 420
- "A standalone client application not under a SAP system ID" on page 421
- "A Web services client packaged in its own JAR file" on page 423
- "A deployable client application" on page 424

File changes in the SAP NetWeaver applications directory

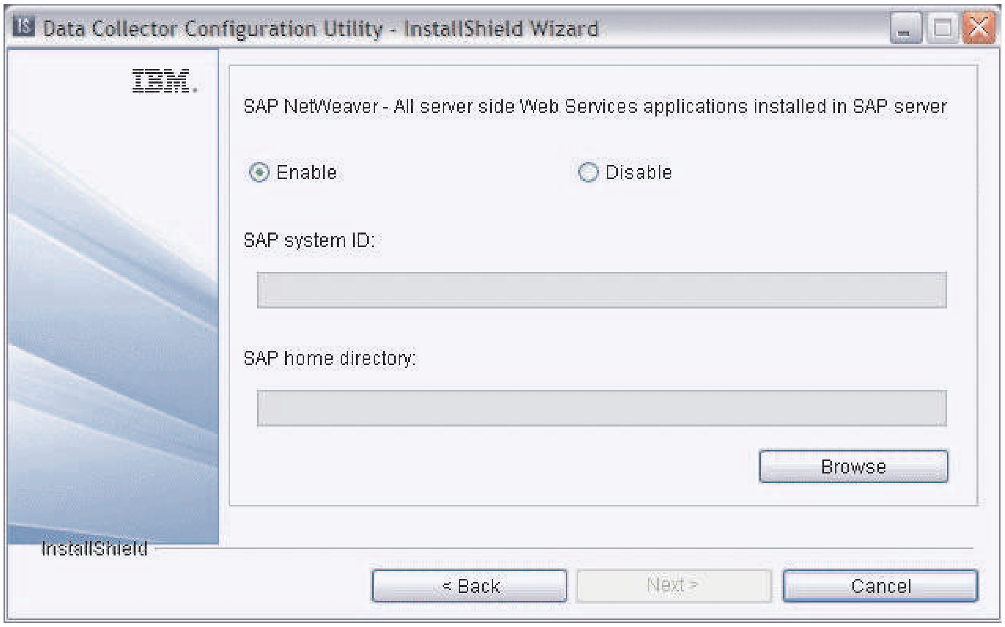
If you use the Data Collector Configuration utility or the `KD4configDC` command to enable or disable data collection for your application server, certain changes are made to files in your SAP applications directory, and the undeploy operation of the SAP administration utilities might not remove all of those changed files. To ensure that upgraded versions of your applications deploy successfully, check the directory for each application after undeploying and delete any residual files that you might not have been expecting. You must enable upgraded applications for data collection again using the Data Collector Configuration utility or the `KD4configDC` command if they were not manually enabled during the upgrade.

All server applications under a SAP system ID

If you have a number of services applications under a common SAP system ID, you can enable all of them for data collection at the same time. You can specify the SAP home directory and the SAP system ID to confirm that the directory corresponding to the SAP system ID exists under the home directory. All services applications that are found under the SAP system ID are enabled. This method also performs some error checking to assist you.

To enable data collection for all server applications under a specific SAP system ID, complete these steps:

- Using the Data Collector Configuration utility:
  1. Stop the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
  2. Run the Data Collector Configuration utility (see "Running the Data Collector Configuration utility" on page 378):



Data Collector Configuration Utility - InstallShield Wizard

SAP NetWeaver - All server side Web Services applications installed in SAP server

● Enable ○ Disable

SAP system ID:

SAP home directory:

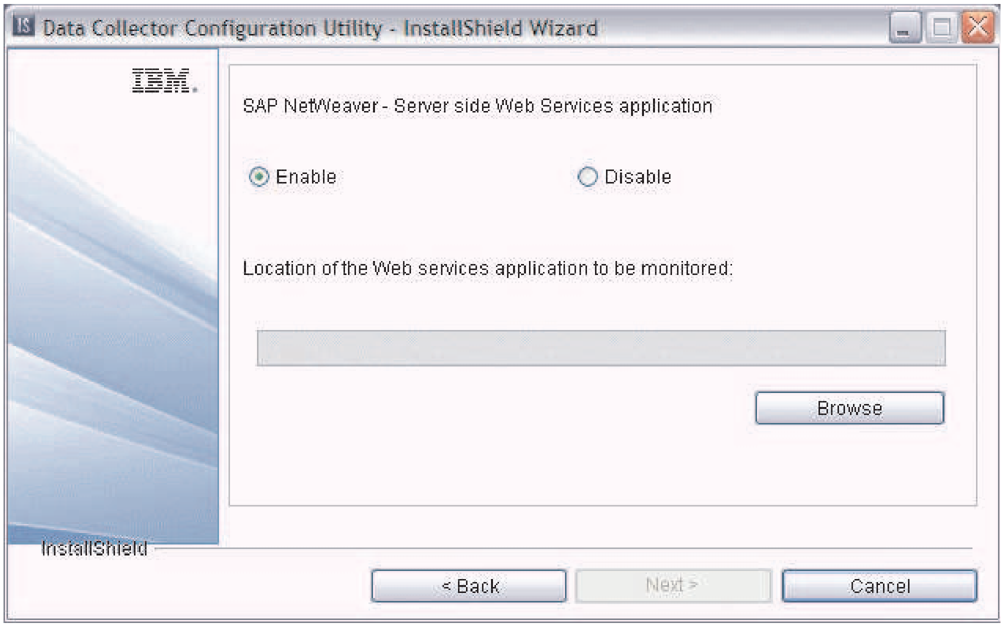
Figure 60. Enabling data collection for all servers under a SAP NetWeaver system ID

     a. Select the SAP NetWeaver runtime environment.
     b. Select the **All server side Web Services applications installed in SAP server** option.
     c. Select the option to enable data collection.
     d. Specify the SAP system ID, for example, `j2e`.
     e. Specify the directory path for the SAP NetWeaver home directory, typically `/usr/sap` or `C:\usr\sap`, though it might reside on any drive.
     f. Wait for the configuration utility to complete the operation.
     g. Exit the utility.
  3. Restart the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
- Using the KD4configDC command:
  1. Stop the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
  2. Run the **`KD4configDC`** command with the `-sid` parameter to enable for data collection all of the services applications found under a commons SAP system ID. Be sure to specify the SAP NetWeaver home directory, and the SAP system ID (see "Enabling data collection using the KD4configDC command" on page 424).
  3. Restart the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.

A server application not located under a SAP system ID

To enable data collection for a server application not located under a SAP system ID, complete these steps:

- Using the Data Collector Configuration utility:
  1. Stop the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
  2. Run the Data Collector Configuration utility (see “Running the Data Collector Configuration utility” on page 378):



Data Collector Configuration Utility - InstallShield Wizard

SAP NetWeaver - Server side Web Services application

● Enable ○ Disable

Location of the Web services application to be monitored:

Figure 61. Enabling data collection on a SAP NetWeaver server-side application

  a. Select the SAP NetWeaver runtime environment.
  b. Select the **Server side Web Services application** option.
  c. Select the option to enable data collection.
  d. Specify the directory path for the location of the services application to be monitored.
  e. Wait for the configuration utility to complete the operation.
  f. Exit the utility.
  3. Restart the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
- Using the `KD4configDC` command:
  1. Stop the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
  2. Run the `KD4configDC` command with the `-sapappsdir` parameter to enable the application for data collection (see “Enabling data collection using the KD4configDC command” on page 424).
  3. Restart the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
- Enabling data collection manually:
  1. Add the `kd4dcagent.jar` and `ibm-jaxrpc-client.jar` files to your application, typically in the `/WEB-INF/lib` directory. If your application uses a

Sun distribution of Java 1.4.2, you must also add xercesImpl.jar and xml-apis.jar. All of these jar files are provided in the KD4/lib directory.

2. Add the ITCAM for SOA servlet filter to the web.xml file for the application, similar to the following example:

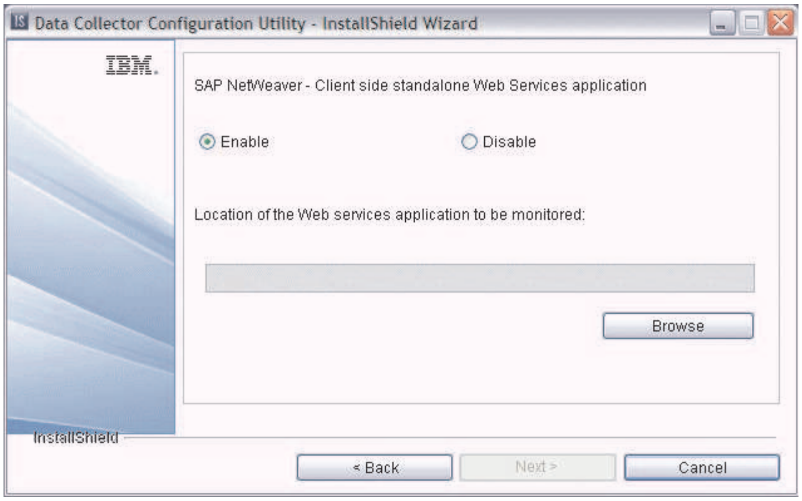
```
<?xml version="1.0" encoding="UTF-8"?>
<web-app>
  <display-name>SayHelloWS_Config1.war</display-name>
  <servlet>
    <servlet-name>SayHelloWS_Config1_SoapServlet</servlet-name>
    <display-name>SayHelloWS_Config1_SoapServlet</display-name>
       <servlet-class>SoapServlet</servlet-class>
    <load-on-startup>0</load-on-startup>
  </servlet>
  <servlet-mapping>
    <servlet-name>SayHelloWS_Config1_SoapServlet</servlet-name>
    <url-pattern>/*</url-pattern>
  </servler-mapping>
  <session-config>
    <session-timeout>1</session-timeout>
  </session-config>
  <filter>
    <filter-name>KD4ServletFilter</filter-name>
    <filter-class>com.ibm.management.soa.agent.sap.WebServiceFilter
    </filter-class>
  </filter>
  <filter-mapping>
     <filter-name> KD4ServletFilter</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping></web-app>
```

3. Install your upgraded application into your application server.

A standalone client application not under a SAP system ID

To enable data collection for a standalone client application not located under a SAP system ID, complete these steps:

- Using the Data Collector Configuration utility:
  1. Run the Data Collector Configuration utility (see “Running the Data Collector Configuration utility” on page 378):



SAP NetWeaver - Client side standalone Web Services application

● Enable ○ Disable

Location of the Web services application to be monitored:

Figure 62. Enabling data collection on a SAP NetWeaver standalone client side application

     a. Select the SAP NetWeaver runtime environment.

   b. Select the **Client side standalone Web Services application** option.
   c. Select the option to enable data collection.
   d. Specify the directory path for the location of the services application to be monitored.
   e. Wait for the configuration utility to complete the operation.
   f. Exit the utility.
2. Modify the classpath used to launch the standalone application to include the kd4dcagent.jar file, which is provided in the /KD4/lib directory.
3. Run the application.

- Using the KD4configDC command:
  1. Run the KD4configDC command with the -clientappsdir parameter to enable the application for data collection (see "Enabling data collection using the KD4configDC command" on page 424).
  2. Modify the classpath used to launch the standalone application to include the kd4dcagent.jar file, which is provided in the /KD4/lib directory.
  3. Run the application.
- Enabling data collection manually:
  1. Modify the classpath used to launch the standalone application to include the kd4dcagent.jar file, which is provided in the /KD4/lib directory:
  2. Update the lports_1.xml file to define the feature needed for the ITCAM for SOA protocol, similar to the following example (see the text in **bold** type):

```
<?xml version="1.0" encoding="UTF-8"?>
<LogicalPorts Name='CalculatorServer'
InterfaceName='test.proxy.CalculatorServer'>
<LogicalPort Name='Config1Port_Document'
  Endpoint='http://tive10:50000/CalculatorServer
    /Config1?style=document'
  BindingName='Config1Binding'
  BindingUri='urn:CalculatorServerWsd/Config1/document'
  BindingImplementation='SOAP 1.1 HTTP Binding with Attachments'
  StubName='test.proxy.Config1BindingStub' Default='true'
  InterfaceName='test.proxy.CalculatorServerViDocument'
  Original='true' Valid='true'>
<globalFeatures>
  <Feature Name='http://www.sap.com/webas/630/soap/features
    /authentication' Provider='SecurityProtocol' Original='true'>
    <Property Name='AuthenticationLevel' Value='None'>
    </Property>
    <Property Name='AuthenticationMechanism' Value='None'>
    </Property>
  </Feature>
  <Feature Name='http://www.sap.com/webas/630/soap/features
    /transportguarantee' Original='true'>
    <Property Name='Level' Value='No'></Property>
  </Feature>
  <Feature Name='http://www.sap.com/webas/630/soap/features/headers/'
    Provider='SoapHeadersProtocol' Original='false'>
  </Feature>
  <Feature Name='http://www.sap.com/webas/630/soap/features/session/'
    Provider='SessionProtocol' Original='false'>
    <Property Name='SessionMethod' Value='httpCookies'>
    </Property>
  </Feature>
  <Feature Name=' http://www.ibm.com/tivoli/itcam4soa//'
    Provider='KD4Protocol' Original='false'>
    <Property Name='portName' Value='Config1Port_Document'>
    </Property>
  </Feature>  </globalFeatures>
  <localFeatures>
```

```
    <Operation Name='add'>
    </Operation>
    <Operation Name='divide'>
    </Operation>
    <Operation Name='multiply'>
    </Operation>
    <Operation Name='subtract'>
    </Operation>
  </localFeatures>
</LogicalPort>
</LogicalPorts>
```

3. Update the `protocols.txt` file to declare the ITCAM for SOA protocol, similar to the following example (see the text in **bold** type):

```
#Default Protocol implementations
#Fri Nov 18 13:54:53 GMT+08:00 2005
SessionProtocol=com.sap.engine.services.webservices.jaxrpc
  .wsdl2java.features.builtin.SessionProtocol
MessageIdProtocol=com.sap.engine.services.webservices.jaxrpc
  .wsdl2java.features.builtin.MessageIdProtocol
SecurityProtocol=com.sap.security.core.client.ws.SecurityProtocol
SoapHeadersProtocol=com.sap.engine.services.webservices.jaxrpc
  .wsdl2java.features.builtin.SoapHeadersProtocol
KD4Protocol= com.ibm.management.soa.agent.sap.ITCAMClientProtocol
```

4. Deploy your upgraded application.

A Web services client packaged in its own JAR file

To enable data collection for a Web services client packaged in its own JAR file but being used by a WAR, complete these steps:

1. Modify the classpath for the application to include the `kd4dcagent.jar` file. This jar is provided in the `/KD4/lib` directory.
2. Do one of the following tasks to enable data collection:
   - Using the Data Collector Configuration utility:
     a. Run the Data Collector Configuration utility (see "Running the Data Collector Configuration utility" on page 378)
     b. Select the SAP NetWeaver runtime environment.
     c. Select the **Client side standalone Web Services application** option.
     d. Select the option to enable data collection.
     e. Specify the directory path for the location of the services application to be monitored. Because your standalone client application is a .jar file, be sure to specify the full directory path for the location of the .jar file.
     f. Wait for the configuration utility to complete the operation.
     g. Exit the utility.
   - When using the `KD4configDC` command, run the `KD4configDC` command with the `-clientappsdir` parameter to enable the application for data collection (see "Enabling data collection using the KD4configDC command" on page 424). Because your standalone client application is a .jar file, be sure to specify the full directory path for the location of the .jar file.
   - To enable data collection manually, add the ITCAM for SOA protocol to the appropriate deployment descriptors as described in manual steps 2 on page 422 and 3 for the standalone client application.
3. Install your upgraded application into your application server.

A deployable client application

To enable data collection for a deployable client application such as a JSP or another service, complete the following steps:

1. You do not need to stop the SAP NetWeaver application server if it is already running.
2. Manually add the `kd4dcagent.jar` file to the `\lib` directory for the application.
3. Manually modify `application-j2ee-engine.xml`, adding the following reference shown in bold text:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <!DOCTYPE application-j2ee-engine SYSTEM "application-j2ee-engine.dtd">
   <application-j2ee-engine>
    <reference
     reference-type="hard">
     <reference-target
      provider-name="sap.com"
      target-type="application">MathDepProxy</reference-target>
    </reference>
    <reference reference-type="hard">
     <reference-target provider-name="sap.com"
   target-type="library">sapxmltoolkit</reference-target>
    </reference>
    <provider-name>sap.com</provider-name>
    <fail-over-enable
     mode="disable"/>
   </application-j2ee-engine>
   ```

4. Manually modify the application code to add the ITCAMClientProtocol protocol to the protocol list for each of your client stubs.

   Following is an example of how to modify a deployable client side application:

   ```
   // initialization of the web service client
   .....
   // create a deployable proxy object.
   SystemDetail service = new SystemDetailImpl();
   SystemDetailViDocument port = service.getLogicalPort();
   BaseGeneratedStub stub = (BaseGeneratedStub)port;
   ProtocolList list = stub._getGlobalProtocols();
   ITCAMClientProtocol protocol = new ITCAMClientProtocol();
   list.add(protocol);

   // call web service
   .....
   ```

5. Install your upgraded application into your application server.

Enabling data collection using the KD4configDC command

Run the `KD4configDC` command to enable data collection for your SAP NetWeaver application.

1. Enter the following command:
   - For supported Windows operating systems:

     ```
     KD4configDC.bat -enable -env 6 {-sid home sid |
     -sapappsdir apps_dir | -clientappsdir apps_dir}
     ```

   - For supported AIX, Solaris, HP-UX, and Linux operating systems:

     ```
     KD4configDC.sh -enable -env 6 {-sid home sid |
     -sapappsdir apps_dir | -clientappsdir apps_dir}
     ```

   The following parameters are specified in these commands:

   -enable
   Causes the command to enable the application for data collection.

   -env 6 Defines the environment to be enabled as SAP NetWeaver.

–sid *home sid*
: For this parameter, *home* is the SAP home directory, typically /usr/sap or C:\usr\sap, but it could reside on any drive. The *sid* argument is the SAP system ID. Both of these arguments are used to confirm that the directory corresponding to the specified SID exists under the specified home. All services applications that are found under the SID are enabled. This is the preferred option to specify, because it does the same tasks as –sapappsdir parameter, and some error checking is also performed to assist you.

-sapappsdir *apps_dir*
: Specifies that the directory path specified by *apps_dir* is the location of the services application to be monitored. Use this parameter for a server-side application if your application directory is not located under the SID.

-clientappsdir *apps_dir*
: Specifies that the directory path specified by *apps_dir* is the location of the services application to be monitored. Use this parameter for a stand-alone client application. There is no default path for the –clientappsdir parameter.

  If your standalone client application is a .jar file, be sure to specify the full directory path for the location of the .jar file. See the examples that follow.

apps_dir
: Specifies the directory path of the services application to be monitored.

Examples:

-
  ```
  KD4configDC.bat -enable -env 6 -sid C:\usr\sap j2e
  ```
  In this example, the C:\usr\sap SAP home directory is specified, along with the system ID j2e. All services applications found under this combination of home directory and SID are enabled for data collection.
-
  ```
  KD4configDC.bat -enable -env 6 -sapappsdir /appl1
  ```
  In this example, the services application directory location /appl1 is specified. This parameter might be used for enabling a server side or deployable client side application for data collection.
-
  ```
  KD4configDC.bat -enable -env 6 -clientappsdir /appl2
  ```
  In this example, the services application directory location /appl2 is specified. This command enables the stand-alone client side application for data collection.
-
  ```
  KD4configDC.bat -enable -env 6 -sapappsdir
    "C:\SAP\My Sap\j2e\JC000\j2ee\cluster\server0\apps"
  ```
  In this example, the services application directory is not located under the SID home. The fully qualified directory path of the services application is specified. This example also shows the directory path surrounded by quotation marks, which are needed if the path contains one or more blank characters.
-
  ```
  KD4configDC.sh -enable -env 6 -clientappsdir /opt/IBM/appsdir
  ```
  In this example, the KD4configDC command is run on a supported AIX, Solaris, HP-UX, or Linux operating systems.

-

  ```
  KD4configDC.sh -enable -env 6 -clientappsdir
    /usr/sap/Customer/EnterpriseSTDClientProxy.jar
  ```

  In this example, the stand-alone client application is a .jar file, so the full directory path location of the file is specified.

Disabling data collection

To disable the SAP NetWeaver application for data collection, depending on the type of application, complete the following steps:

- For all server applications under a common SAP system ID:
  1. Stop the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
  2. Disable data collection for the SAP NetWeaver environment by running either the Data Collector Configuration utility or the **`KD4configDC`** command.
     - Using the Data Collector Configuration utility:
       a. Select the SAP NetWeaver runtime environment.
       b. Select the **All server side Web Services applications installed in SAP server** option.
       c. Select the option to disable data collection.
       d. Specify the SAP system ID.
       e. Specify the SAP home directory.
       f. Wait for the configuration utility to complete the operation.
       g. Exit the utility.
     - Using the `KD4configDC` command: See "Disabling data collection using the KD4configDC command" on page 427). Specify the `–sid` parameter along with the SAP home directory and SAP system ID.
  3. Restart the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
- For a server application:
  1. Stop the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
  2. Disable data collection for the SAP NetWeaver environment by running either the Data Collector Configuration utility or the `KD4configDC` command.
     - Using the Data Collector Configuration utility:
       a. Select the SAP NetWeaver runtime environment.
       b. Select the **Server side Web Services application** option.
       c. Select the option to disable data collection.
       d. Specify the directory path for the location of the services application to be monitored.
       e. Wait for the configuration utility to complete the operation.
       f. Exit the utility.
     - Using the `KD4configDC` command: See "Disabling data collection using the KD4configDC command" on page 427. Specify the `–sapappsdir` parameter.
  3. Restart the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.

  If you manually enabled the server application for the data collector: Remove the `kd4dcagent.jar` and `ibm-jaxrpc-client.jar` files from your application classpath, along with the `xercesImpl.jar` and `xml-apis.jar` files if your application uses a Sun distribution of Java 1.4.2. Remove the changes you made to the `web.xml` file during the manual enable process. Then reinstall your application into the application server.

- For a stand-alone client application:
  1. Disable data collection for the SAP NetWeaver environment by running either the Data Collector Configuration utility or the **`KD4configDC`** command.
     - Using the Data Collector Configuration utility:
       a. Select the SAP NetWeaver runtime environment.
       b. Select the **Client side standalone Web Services application** option.
       c. Select the option to disable data collection.
       d. Specify the directory path for the location of the services application to be monitored.
       e. Wait for the configuration utility to complete the operation.
       f. Exit the utility.
     - Using the `KD4configDC` command: See "Disabling data collection using the KD4configDC command." Specify the `–clientappsdir` parameter.
  2. Modify the classpath used to launch the stand-alone client application to remove the `kd4dcagent.jar` file.
  3. Run the application.

  If you manually enabled the stand-alone client application for the data collection: Remove the `kd4dcagent.jar` file from the classpath, and remove the changes you made to the `lports_1.xml` and `protocols.txt` files during the manual enable process. Then reinstall your application into the application server.
- For a deployable client application:
  1. You do not need to stop the SAP NetWeaver application server if it is already running.
  2. Manually remove the modifications you made to the application code when you enabled the application for data collection.
  3. Remove the `kd4dcagent.jar` file from the deployable client application.
  4. Redeploy the application.

Disabling data collection using the KD4configDC command

Run the `KD4configDC` command to disable the application for the data collector:

- For supported Windows operating systems:
```
KD4configDC.bat -disable -env 6 {–sid home sid |
–sapappsdir apps_dir | –clientappsdir apps_dir}
```
- For supported AIX, Solaris, HP-UX, and Linux operating systems:
```
KD4configDC.sh -disable -env 6 {–sid home sid |
–sapappsdir apps_dir |  –clientappsdir apps_dir}
```

The following parameters are specified in these commands:

-disable
Causes the command to disable the data collector for the specified environment.

-env 6 Defines the environment to be disabled as SAP NetWeaver.

–sid *home sid*
For this parameter, *home* is the SAP home directory, typically `/usr/sap` or `C:\usr\sap`, but it could reside on any drive. The <*sid*> argument is the

SAP system ID. Both of these arguments are used to confirm that the directory corresponding to the specified SID exists under the specified home. All services applications that are found under the SID are disabled. This is the preferred option to specify, because it does the same tasks as the `–sapappsdir` parameter, and some error checking is also performed to assist you.

-sapappsdir
Specifies that the directory path specified by `apps_dir` is the location of the services application being monitored. Use this parameter for either a server-side application or a deployable client-side application.

-clientappsdir
Specifies that the directory path specified by `apps_dir` is the location of the services application being monitored. Use this parameter for a stand-alone client-side application. There is no default path for the `–clientappsdir` parameter.

If your stand-alone client application is a .jar file, be sure to specify the full directory path for the location of the .jar file. See the examples that follow.

apps_dir
Specifies the directory path of the services application being monitored.

Examples:

-
  ```
  ./KD4configDC.sh -disable -env 6 -sid /usr/sap J2E
  ```
  In this example, *SAP_HOME* and the SAP system name are provided to disable the application for the data collector. The /usr/sap directory is the directory where SAP NetWeaver is installed. `J2E` is the SAP system name.
-
  ```
  KD4configDC.bat -disable -env 6 -sapappsdir /appl1
  ```
  In this example, the services application directory location */appl1* is specified. This parameter might be for disabling a server-side or deployable client-side application.
-
  ```
  KD4configDC.bat -disable -env 6 -clientappsdir /appl2
  ```
  In this example, the services application directory location */appl2* is specified. This command disables a stand-alone client-side application.
-
  ```
  KD4configDC.bat -disable -env 6 -sapappsdir
    "C:\SAP\My Sap\j2e\JC000\j2ee\cluster\server0\apps"
  ```
  In this example, the services application directory is not located under the SID home. The fully qualified directory path of the services application is specified. This example also shows the directory path surrounded in quotation marks, which must be used if the path contains blank spaces.
-
  ```
  KD4configDC.sh -disable -env 6 -clientappsdir
    /usr/sap/j2e/JC000/j2ee/cluster/server0/apps
  ```
  In this example, the `KD4configDC` command is run on a supported AIX, Solaris, HP-UX, or Linux operating systems.
-
  ```
  KD4configDC.sh -disable -env 6 -clientappsdir
    /usr/sap/Customer/EnterpriseSTDClientProxy.jar
  ```

In this example, the stand-alone client application is a .jar file, so the full directory path location of the file is specified.

Additional considerations

As you enable SAP NetWeaver applications for the data collector, keep in mind these additional considerations:

- In the Tivoli Enterprise Portal, the display pattern for server instances is `D4:`*`hostname-SID_instance_server`*. This format displays each server uniquely in the Tivoli Enterprise Portal.

  For example, suppose there are two different SAP NetWeaver servers, `server1` and `server2`, on the same computer system:

  - The hostname of the system is `tiv121`.
  - The SID for both servers is `J2E`
  - The instance for both servers is `00`

  These two servers are each displayed uniquely in the Tivoli Enterprise Portal as `D4:tiv121-J2E_00_S0` and `D4:tiv121-J2E_00_S1`.
- ITCAM for SOA uses the service port name to identify services. If you have two or more service ports deployed that have the same name, these will appear to be the same service port in the Tivoli Enterprise Portal displays.
- The first time that the service is called, there might be a delay of several seconds due to the data collector loading the WSDL related information for the service. On subsequent calls of the service, however, data is retrieved as expected.
- When you enable and disable data collection for your applications, the configuration file is automatically backed up.
  - For a server application, the `web.xml` file is backed up in the same directory where it is currently located. For example, if the original `web.xml` file is located in *`apps_dir`*`/app01/web.xml`, the file is backed up to *`apps_dir`*`/app01/web.xml.kd4backup.`*`timestamp`*, where *timestamp* is a timestamp for when the backup is performed.
  - For a standalone client application that is not a JAR file, the `lport_1.xml` file is backed up in the same directory where it is currently located. For example, if the original `lport_1.xml` file is located in *`standalone_dir`*`/lport_1.xml`, the file is backed up to *`standalone_dir`*`/lport_1.xml.kd4backup.timestamp`, where *timestamp* is a timestamp for when the backup is performed.
  - For a standalone client application that is a JAR file, the `lport_1.xml` file is backed up as `lport_1.xml.kd4backup.`*`timestamp`*, and packed into the JAR file.

  If you experience errors after enabling or disabling your applications for data collection, you can restore the backed up configuration file manually.

For information about monitoring and managing your services in a SAP NetWeaver application server runtime environment, see the *IBM Tivoli Composite Application Manager for SOA User's Guide*.

Chapter 16. Configuring data collection: WebSphere Community Edition

This section describes the support for the monitoring of services flows in a WebSphere Community Edition (CE) Java EE Application Server environment.

The list of versions of WebSphere Community Edition supported by ITCAM for SOA 7.2 Fix Pack 1 is available from the Software product compatibility reports website. For information about accessing reports from this website, see "Required software" on page 15.

In general, the data collector for the WebSphere CE environment operates in the same way as the WebSphere Application Server, BEA WebLogic Server, and JBoss environments. The same types of log files are used, messages are filtered in a similar fashion, and performance is comparable. WebSphere CE server instances are identified in the Tivoli Enterprise Portal navigator view in the form ofd4::*hostname-port*.

You run the `KD4configDC` command once to enable all available WebSphere CE applications for monitoring. If additional applications are added to the environment after running the `KD4configDC` command, you must run it again to recognize the newly added applications. Applications that are already enabled are not affected.

Important:

- You cannot use the Data Collector Configuration utility to configure data collection for WebSphere CE.
- The option to configure data collection for WebSphere Community Edition is not available on Solaris platforms.

Enabling WebSphere CE applications for data collection

To enable WebSphere CE applications for data collection, complete the following steps:

1. Before enabling the application for data collection, increase the WebSphere CE JVM maximum heap size (Xmx) to 256 MB, and the JVM maximum permanent generation size (MaxPermSize) to 128 MB. You can set these values in the JAVA_OPTS keyword:
   - For supported Windows operating systems, edit the *WASCE_HOME*\bin\setenv.bat script file:

     ```
     set JAVA_OPTS=-Xms128m -Xmx256m -XX:PermSize=64m -XX:MaxPermSize=128m
     "-Djava.endorsed.dirs=%GERONIMO_BASE%/lib/endorsed" %JAVA_OPTS%
     ```

   - For supported AIX and Linux operating systems, edit the *WASCE_HOME*/bin/setenv.sh script file:

     ```
     export JAVA_OPTS=-Xms128m -Xmx256m -XX:PermSize=64m -XX:MaxPermSize=128m
     -Djava.endorsed.dirs=$GERONIMO_BASE/lib/endorsed %JAVA_OPTS%
     ```

2. Ensure that the application server is running before enabling the application for data collection. Follow the procedures in your WebSphere CE documentation for starting the server.

3. (Optional) Run the KD4configDC command using the –list parameter to create a list of applications to be enabled with subsequent runs of the KD4configDC command.
4. (Optional) Review and manually modify the file (specified by the –file *filename* argument specified when you ran the KD4configDC command) containing the list of applications to be enabled, to exclude those applications that must not be enabled.
5. Run the KD4configDC command again to enable the applications in the file list, this time not specifying the –list parameter. As a result of enabling the applications, each Java EE services application is redeployed automatically.
6. During this process, each Java EE application is backed up as *name*.*date*.*hour*.min.*sec*.bak.*type* (where *type* is the file type, such as jar, war, or ear), and stored in the *WASCE_HOME*/temp/KD4 directory, where *WASCE_HOME* is the location where WebSphere CE is installed.

   These backup files are not automatically removed during the enable or disable process. You should consider removing them when they are no longer needed, to conserve available disk storage.

Running the KD4configDC command

Run the KD4configDC command to enable the application for data collection:

- For supported Windows operating systems:

  ```
  KD4configDC.bat –enable –env 7 {WASCE_HOME}
     –user user name –passwd password [–list] –file filename
  ```
- For supported AIX and Linux operating systems:

  ```
  KD4configDC.sh –enable –env 7 {WASCE_HOME}
     –user user name –passwd password [–list] –file filename
  ```

The following parameters are specified in these commands:

–enable
Causes the command to enable the application for the specified environment.

–env 7 Defines the application server runtime environment for which the application is enabled as WebSphere CE.

WASCE_HOME
This is an optional parameter that specifies the directory path where WebSphere CE is installed. If you have already created a WASCE_HOME system environment variable, then this parameter is not required. Typical values for this variable are:

- For supported Windows operating systems:

  ```
  C:\Program Files\IBM\WebSphere\AppServerCommunityEdition
  ```
- For supported AIX and Linux operating systems:

  ```
  /opt/IBM/WebSphere/AppServerCommunityEdition
  ```

–user *user name*
Specifies a valid WebSphere CE user name that has administrator authority. See your WebSphere CE documentation for more information about creating Administrator user names and passwords. See your local system administrator for assistance, if needed.

–passwd *password*
Specifies a valid password that is associated with the specified WebSphere CE user name. See your WebSphere CE documentation for more

information about creating administrator user names and passwords. See your local system administrator for assistance, if needed.

–list This is an optional parameter that, when specified, causes the utility to create a list of available applications that can be later enabled or disabled, and store this list in the specified file name indicated by the `–file` *filename* parameter. The specified enable or disable operation is *not* performed at this time, only the file is created for future enable or disable operations (in this special case you must specify either the `–enable` or `–disable` parameter in the command, but it is ignored).

You should examine this file and modify it as needed to exclude certain applications from the list that you do not want to enable or disable with subsequent runs of the `KD4configDC` command.

If your application deployed with an external plan file, the application is redeployed as part of the enable or disable operation, so you should exclude that application from the list.

Subsequent runs of the `KD4configDC` command use the list of files in the specified *filename* until you overwrite the contents of the file with another command using the`–list` parameter.

–file *filename*

This parameter is used in two different ways, depending on whether the `–list` parameter is also specified in the `KD4configDC` command:

- If the `–list` parameter is specified, the file name indicated by *filename* is created relative to the current directory location. For example, if you navigated to `/KD4/bin` to run the `KD4configDC` command, this file is created in that directory. You can also specify a fully qualified file and path. All WebSphere CE services applications that are eligible to be enabled or disabled in subsequent runs of the `KD4configDC` command are discovered and listed in the designated file. Note that no enable or disable operation is performed on these applications at this time, only the list is created and stored in the file. When the list is created, you can modify this list manually to exclude applications that you do not want to be enabled or disabled with subsequent runs of the `KD4configDC` command (for example, those deployed with an external plan file).
- If the `–list` parameter is not specified, then it is assumed that this file exists (from a previous run of the `KD4configDC` command) and contains the list of WebSphere CE applications that you want to enable or disable. The `KD4configDC` command reads the file specified by <*filename*> and performs the enable or disable operation on each application that is not already enabled or disabled.

  Applications in the list that are already enabled or disabled are not changed. A message is displayed indicating that they are ignored for this operation.

If the specified file name exists, it is overwritten.

Do not use reserved file names. When you specify the file name to be created with the `–list –file` *filename* parameters, do not use the name of a reserved file that is already in the current directory. For example, if you are in the `\KD4\bin` directory, do not use existing file names, such as `KD4configDC.bat`, or `configWASCEDC.bat`. This overwrites these files and cause errors in operation, and you must recover these files from the installation media.

You should either specify a fully qualified unique file and directory path, create a separate folder for this file within the current directory, or create a unique file name and use it consistently each time when you run the KD4configDC command using the –list parameter. If you use different file names with different runs of the KD4configDC command, they are all stored in the current directory and you must keep track of which file to specify in subsequent enable or disable operations.

Examples:

-
```
KD4configDC.bat –enable –env 7 C:\WASCE –user system -passwd manager
  –list –file filelist01
```
  In this example, the value of WASCE_HOME has been provided, along with a valid user name and password. Because the –list parameter is specified, the utility initiates a discovery of the eligible WebSphere CE applications that can be enabled or disabled with later runs of the KD4configDC command, and writes that list to the file name filelist01 in the current directory. Even though the –enable parameter is specified, it is ignored for this command and no applications are enabled.

  After this command completes, you have the opportunity to manually modify this file and remove any applications that you do not want to be enabled or disabled with subsequent runs of the KD4configDC command.

-
```
KD4configDC.bat –enable –env 7 C:\WASCE –user system -passwd manager
  –list –file files\filelist01
```
  In this example, the list of eligible files is stored in filelist01, which is created in the \files folder under the current directory. Specifying a separate folder might be a good practice to avoid potentially writing over existing reserved files in the current directory.

-
```
KD4configDC.bat –enable –env 7 C:\WASCE –user system -passwd manager
  –list –file "D:\WASCE files\filelist01"
```
  In this example, the list of eligible files is stored in filelist01, which is created in the \WASCE files folder on the D: drive. This example shows that you can specify a fully qualified file name and path for the file list. Also, if the fully qualified path contains a blank character, the path is surrounded with quotation marks.

-
```
KD4configDC.bat –enable –env 7 C:\WASCE –user system -passwd manager
  –file filelist01
```
  In this example, the –list parameter is not specified, and now KD4configDC reads the contents of the file filelist01 in the current directory, and performs the enable operation on all applications in the list that are not already enabled for this data collector. If an application in the list is already enabled, it is ignored and its state is not changed. If an application is specified in the list that cannot be found, a message is displayed and the command continues to the next application in the file. If the specified file is not found in the current directory, an error message is displayed.

-
```
KD4configDC.bat -enable -env 7 -user cde321 -passwd xxx111xxx –file filelist01
```
  In this example, the WASCE_HOME environment variable has been set, and is used by default when the command is run.

-

```
KD4configDC.bat –enable –env 7
  "C:\Program Files\IBM\WebSphere\AppServerCommunityEdition"
  –user abc123 -passwd xyz010 –file filelist01
```

In this example, the value of WASCE_HOME is specified, and because it includes a blank space, is surrounded with quotation marks.

-

```
KD4configDC.sh -enable -env 7 /opt/IBM/WebSphere/AppServerCommunityEdition
   -user user1 -passwd zz11zz –file filelist01
```

In this example the KD4configDC command is run on a supported AIX or Linux operating system.

Enabling data collection manually

You might have used a custom plan file to deploy your WebSphere CE application. If so, then you need to perform some additional manual steps to enable these WebSphere CE applications for data collection:

1. If you have not run the KD4configDC command to enable other WebSphere CE applications that use the default plan file, you must run the KD4configDC command (using the procedure described in the previous section) once to place the necessary JAR files into their correct locations. Specify an empty file as the value for the –file parameter. This results in the message KD4CF0038E being displayed, indicating that there are no applications to be enabled. You can ignore this message.

   If you have already run the KD4configDC command for at least one WebSphere CE application that uses the default plan file, then this step is already completed and you do not need to run the utility again.

2. Edit the custom deployment plan file. Within each <web-app> or <openejb-jar> element, add the following <dependency> and <hidden-classes> elements:

   ```
   <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
   <uri>KD4/kd4dcagent/6.0/jar</uri>
   </dependency>
   <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
   <uri>KD4/ibm-jaxrpc-client/6.0.2/jar</uri>
   </dependency>
   <hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
   <filter>com.ibm.wsdl</filter>
   </hidden-classes>
   <hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
   <filter>javax.wsdl.factory.WSDLFactory</filter>
   </hidden-classes>
   ```

   The following example shows how to add *<dependency>* and *<hidden-classes>* elements within a *<web-app>* element:

   ```
   <web-app xmlns="http://geronimo.apache.org/xml/ns/web"
       xmlns:sys="http://geronimo.apache.org/xml/ns/deployment-1.0"
       xmlns:naming="http://geronimo.apache.org/xml/ns/naming-1.0"
       xmlns:security="http://geronimo.apache.org/xml/ns/security-1.0"
           configId="com/ibm/j2g/webservices.war">
        <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
        <uri>KD4/kd4dcagent/6.0/jar</uri>
    </dependency>
    <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
        <uri>KD4/ibm-jaxrpc-client/6.0.2/jar</uri>
    </dependency>
    <hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
        <filter>com.ibm.wsdl</filter>
    </hidden-classes>
    <hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
        <filter>javax.wsdl.factory.WSDLFactory</filter>
    </hidden-classes>
   ```

```
<context-root>/webservices</context-root>
<context-priority-classloader>false</context-priority-classloader>
</web-app>
```

The following example shows how to add *<dependency>* and *<hidden-classes>* elements within an *<openejb-jar>* element:

```
<openejb-jar xmlns="http://www.openejb.org/xml/ns/openejb-jar"
       configId="com/ibm/dw/bookshop" parentId="BookShopDB">
     <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
         <uri>KD4/kd4dcagent/6.0/jar</uri>
     </dependency>
     <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
         <uri>KD4/ibm-jaxrpc-client/6.0.2/jar</uri>
     </dependency>
     <hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
        <filter>com.ibm.wsdl</filter>
     </hidden-classes>
     <hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
        <filter>javax.wsdl.factory.WSDLFactory</filter>
     </hidden-classes>

   <enterprise-beans>
       <entity>
          <ejb-name>CategoryBean</ejb-name>
          <jndi-name>CategoryBean</jndi-name>
           <table-name>categories</table-name>
            <cmp-field-mapping>
               <cmp-field-name>catId</cmp-field-name>
               <table-column>catId</table-column>
             </cmp-field-mapping>
           <cmp-field-mapping>
           <cmp-field-name>name</cmp-field-name>
               <table-column>name</table-column>
             </cmp-field-mapping>
          <resource-ref>
               <ref-name>jdbc/basic/BookShopDatabase</ref-name>
               <application>null</application>
               <module>BooksShopDB</module>
               <name>BookShopDBPool</name>
             </resource-ref>
       </entity>
   </enterprise-beans>
</openejb-jar>
```

3. Add the ITCAM for SOA server-side handler to all of the handler chains in the webservices.xml files within the application (if the application does not contain `webservices.xml`, skip this step).

   Modify the `webservices.xml` files by adding the following lines:

```
<handler>
    <handler-name>KD4ServerHandler</handler-name>
    <handler-class>
      com.ibm.management.soa.agent.wasce.ITMWASCEServerHandler
    </handler-class>
</handler>
```

   The following example shows how to add the server-side handler to the `webservices.xml` file:

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices xmlns="http://java.sun.com/xml/ns/j2ee" version="1.1">
    <webservice-description>
        <webservice-description-name>SearchPhones</webservice-description-name>
        <wsdl-file>WEB-INF/wsdl/search-phones-service.wsdl</wsdl-file>
        <jaxrpc-mapping-file>
          WEB-INF/search-phones-server-mapping.xml
        </jaxrpc-mapping-file>
        <port-component>
            <port-component-name>SearchPhonesService</port-component-name>
            <wsdl-port>SearchPhonesService</wsdl-port>
            <service-endpoint-interface>
              com.ibm.j2g.webservices.server.SearchPhonesPortType
            <service-endpoint-interface>
            <service-impl-bean>
                <servlet-link>SearchPhonesServer</servlet-link>
            </service-impl-bean>
            <handler>
              <handler-name>KD4ServerHandler</handler-name>
              <handler-class>
                    com.ibm.management.soa.agent.wasce.ITMWASCEServerHandler
                </handler-class>
            </handler>      </port-component>
   </webservice-description>
</webservices>
```

If there are multiple <*port-component*> elements, you must add one <*handler*> element within each <*port-component*> element.

4. If the application contains a web.xml file and the web.xml file includes a <*service-ref*> element, you must add the ITCAM for SOA client handler to the handler chain in the web.xml file. If there is no web.xml file or an existing web.xml file does not include a <*service-ref*> element, skip this step.

   Modify the web.xml file by adding the following lines:

```
<handler>
    <handler-name>ClientHandler</handler-name>
    <handler-class>
      com.ibm.management.soa.agent.wasce.ITMWASCEClientHandler
    </handler-class>
</handler>
```

   The following example shows how to add the client handler to the handler chain in the web.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
            http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd" version="2.4">
  <servlet>
    <servlet-name>SearchPhonesServer</servlet-name>
    <servlet-class>
      com.ibm.j2g.webservices.server.SearchPhonesServer
    </servlet-class>
  </servlet>
  <servlet-mapping>
     <servlet-name>SearchPhonesServer</servlet-name>
     <url-pattern>/server</url-pattern>
  </servlet-mapping>
  <service-ref>
     <service-ref-name>service/SearchPhones</service-ref-name>
        <service-interface>
           com.ibm.j2g.webservices.client.SearchPhonesService
        </service-interface>
     <wsdl-file>WEB-INF/wsdl/search-phones-service.wsdl</wsdl-file>
     <jaxrpc-mapping-file>
        WEB-INF/search-phones-client-mapping.xml
     </jaxrpc-mapping-file>
     <handler>
        <handler-name>KD4ClientHandler</handler-name>
        <handler-class>
           com.ibm.management.soa.agent.wasce.ITMWASCEClientHandler
        </handler-class>
      </handler>
    </service-ref>
  </web-app>
```

5. If the application contains the `ejb-jar.xml` file and the `ejb-jar.xml` file includes the *<service-ref>* element, you must add the ITCAM for SOA client handler to the handler chain in `ejb-jar.xml` file. If there is no `ejb-jar.xml` file in the application, or if an existing `ejb-jar.xmll` file does not include the *<service-ref>* element, skip this step.

   The following example shows how to add the client handler to the handler chain in the `ejb-jar.xml` file:

```
<?xml version="1.0" encoding="UTF-8"?>
<ejb-jar xmlns="http://java.sun.com/xml/ns/j2ee" version="2.1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
     http://java.sun.com/xml/ns/j2ee/ejb-jar_2_1.xsd">
   <enterprise-beans>
     <session>
       <ejb-name>BookShopEJB</ejb-name>
       <local-home>com.ibm.dw.bookshop.ejb.BookShopLocalHome</local-home>
      <local>com.ibm.dw.bookshop.ejb.BookShopLocal</local>
      <ejb-class>com.ibm.dw.bookshop.ejb.BookShopBean</ejb-class>
      <session-type>Stateless</session-type>
      <transaction-type>Container</transaction-type>
      <service-ref>
        <service-ref-name>service/Service</service-ref-name>
        <service-interface>javax.xml.rpc.Service</service-interface>
         <wsdl-file>META-INF/wsdl/CurrencyExchangeService.wsdl</wsdl-file>
          <jaxrpc-mapping-file>
             META-INF/client-jaxrpc-mapping.xml
          </jaxrpc-mapping-file>
          <service-qname xmlns:ns=
            "http://www.xmethods.net/sd/CurrencyExchangeService.wsdl">
            ns:CurrencyExchangeService
          </service-qname>
          <handler>
            <handler-name>KD4ClientHandler</handler-name>
            <handler-class>
              com.ibm.management.soa.agent.wasce.ITMWASCEClientHandler
            </handler-class>
          </handler>
        </service-ref>
      </session>
    </enterprise-beans>
 </ejb-jar>
```

6. Redeploy the application into the application server.

Disabling data collection

To disable WebSphere CE applications for data collection, complete the following steps:

1. Ensure that the application server is running.
2. (Optional) Run the `KD4configDC` command using the `–list` parameter to create a list of applications to be disabled with subsequent runs of the `KD4configDC` command.
3. (Optional) Review and manually modify the file containing the list of applications to be disabled, to exclude those applications that should not be disabled.

4. Run the KD4configDC command to disable the applications in the file list. Do not specify the –list parameter. As a result of disabling the applications, each Java EE services application is redeployed automatically.
5. If data collection is disabled for all services applications, do the following:
   a. Shut down the WebSphere CE application server.
   b. Navigate to the *WASCE_HOME*/repository/KD4 directory and manually remove the entire directory and all of its contents.
   c. Restart the WebSphere CE application server.

Running the KD4configDC command

Run the KD4configDC command to disable applications for data collection:

- For supported Windows operating systems:

  ```
  KD4configDC.bat –disable –env 7 {WASCE_HOME} –user user name
    –passwd password [–list] –file filename
  ```

- For supported AIX and Linux operating systems:

  ```
  KD4configDC.sh –disable –env 7 {WASCE_HOME} –user user name
    –passwd password [–list] –file filename
  ```

The parameters specified in these commands are similar to the parameters specified when enabling data collection. See the previous section for details.

Examples:

-
  ```
  KD4configDC.bat –disable –env 7 C:\WASCE –user system -passwd manager
    –list –file filelist01
  ```

  In this example, the value of WASCE_HOME has been provided, along with a valid user name and password. Because the –list parameter is specified, the utility initiates a discovery of the eligible WebSphere CE applications that can be enabled or disabled with later runs of KD4configDC, and writes that list to the file name *filelist01* in the current directory. Even though the –disable parameter was specified, it is ignored for this command and no applications are disabled.

  After this command completes, you have the opportunity to manually modify this file and remove any applications that you do not want to be enabled or disabled with subsequent runs of the KD4configDC command.

-
  ```
  KD4configDC.bat –disable –env 7 C:\WASCE –user system -passwd manager
    –list –file files\filelist01
  ```

  In this example, the list of eligible files is stored in filelist01, which is created in the \files folder under the current directory. Specifying a separate folder might be a good practice to avoid potentially writing over existing reserved files in the current directory.

-
  ```
  KD4configDC.bat –disable –env 7 C:\WASCE –user system -passwd manager
    –list –file "D:\WASCE files\filelist01"
  ```

  In this example, the list of eligible files is stored in filelist01, which is created in the \WASCE files folder on the D: drive. This example shows that you can specify a fully qualified file name and path for the file list. Also, if the fully qualified path contains a blank character, the path is surrounded with quotation marks.

-
  ```
  KD4configDC.bat –disable –env 7 C:\WASCE –user system -passwd manager
    –file filelist01
  ```

In this example, the `–list` parameter is not specified, and now `KD4configDC` reads the contents of the file `filelist01` in the current directory, and performs the disable operation on all applications in the list that are not already disabled for data collection. If an application in the list is already disabled, it is ignored and its state is not changed. If an application is specified in the list that cannot be found, a message is displayed and the command continues to the next application in the file. If the specified file is not found in the current directory, an error message is displayed.

-
  ```
  KD4configDC.bat -disable -env 7 -user cde321 -passwd xxx111xxx –file filelist01
  ```
  In this example, the WASCE_HOME environment variable has been set, and is used by default when the command is run.

-
  ```
  KD4configDC.bat –enable –env 7
    "C:\Program Files\IBM\WebSphere\AppServerCommunityEdition"
    –user abc123 -passwd xyz010 –file filelist01
  ```
  In this example, the value of WASCE_HOME is specified, and, because it includes a blank space, is surrounded with quotation marks.

-
  ```
  KD4configDC.sh -enable -env 7 /opt/IBM/WebSphere/AppServerCommunityEdition
     -user user1 -passwd zz11zz –file filelist01
  ```
  This example is for running `KD4configDC` on a supported AIX or Linux operating system.

Disabling data collection manually

You might have used a custom plan file to deploy your WebSphere CE application. If so, you need to perform some additional manual steps to remove the `<handler>`, `<dependency>`, and `<hidden-classes>` elements that you added manually when the data collector was enabled for these applications. See "Enabling data collection manually" on page 435 for more information on these declarations that were manually added.

If this is the last WebSphere CE application using the data collector for ITCAM for SOA, then after manually removing the elements, run the `KD4configDC` command to remove the associated JAR files from their locations.

After manually disabling the data collector, redeploy the WebSphere CE application.

Additional considerations

When you configure filter controls to block messages, the WebSphere CE data collector only supports the asterisk wild card (*) character in the **IP** field. If you specify a hostname or IP address in that field, the data collector filtering does not match any messages.

Chapter 17. Configuring data collection: DataPower SOA Appliance

This section describes the support for monitoring of service flows through an IBM WebSphere DataPower SOA appliance, where the ITCAM for SOA data collector acts as a proxy between the services clients and servers.

The list of versions of the DataPower SOA appliance supported by ITCAM for SOA 7.2 Fix Pack 1 is available from the Software product compatibility reports website. For information about accessing reports from this website, see “Required software” on page 15.

The DataPower data collector can be integrated with ITCAM for Transactions. If configured, transaction events are sent to a Transaction Collector which stores and aggregates transaction data from multiple data collectors. For more information about configuring the interface to ITCAM for Transactions, see Chapter 18, “Integrating with ITCAM for Transactions,” on page 489.

IBM WebSphere DataPower SOA appliances are used for processing XML messages, and providing message transformation, services acceleration, and security functions. A DataPower appliance is typically used to improve the security and performance of services by offloading functions from the application server that is hosting the target service to a DataPower SOA appliance. Typical functions that are off-loaded include; authentication and authorization, XML schema validation, and services encryption and decryption.

ITCAM for SOA provides a DataPower data collector that operates as a proxy and monitors services flows through a DataPower SOA appliance, providing similar services management and availability information that ITCAM for SOA currently provides for application server runtime environments. This information is displayed in the Tivoli Enterprise Portal using the usual predefined or user-defined workspaces and views.

DataPower supports two proxy types that can process SOA messages:

The Web Services Proxy
You configure a Web Services Proxy by importing one or more WSDL files and then telling the appliance where to direct those messages. Thus, the Web Services Proxy receives only SOAP messages.

The Multi-Protocol Gateway
The Multi-Protocol Gateway is more versatile than the Web Services Proxy. You can use it to process nearly any type of message, including SOAP, non-SOAP XML, text, or binary. For XML messages (including SOAP), XSL transforms are used to manipulate the message. For non-XML messages, similar transform actions can be built using IBM WebSphere Transformation Extender (for more information about this product, see http://www-306.ibm.com/software/integration/wdatastagetx/).

Upgrade your firmware

Before using the DataPower data collector proxy, you must upgrade the firmware on DataPower SOA appliances that you want to monitor, to include the necessary monitoring and data transformation capabilities.

Important:

- Upgrade your firmware to at least version 3.7.1 or later to monitor traffic through the Web Services Proxy.
- Upgrade your firmware to at least version 3.7.1 Fix Pack 4 or later to monitor traffic through a Multi-Protocol Gateway.

Consult your DataPower Appliance documentation for information about upgrading your firmware level.

The DataPower data collector as a proxy

Data collectors provided with ITCAM for SOA are usually installed directly into the application server runtime environment hosting the services being monitored. The DataPower SOA appliance, however, does not support the installation of additional software, such as a data collector. Unlike other application server runtime environments, the ITCAM for SOA data collector for the DataPower environment is installed on a separate computer system and uses a special communication mechanism that allows external software applications to receive data from its internal transaction log.

This communication mechanism is used to retrieve monitoring data about services requests flowing through one or more DataPower SOA appliances, and to convert the data into a format that ITCAM for SOA can process. In this way, the DataPower data collector acts as a proxy between the DataPower SOA appliances and the ITCAM for SOA monitoring agent.

The DataPower data collector can be installed on a dedicated computer system, or it can run on a computer that is also hosting data collectors for other application server runtime environments.

Important: IBM supports only one instance of the DataPower data collector running on any computer system. This one data collector instance, however, can monitor any number of domains on any number of appliances, subject to available resources.

When data collection is enabled for the DataPower environment, the data collector subscribes to each monitored DataPower SOA appliance and then polls the appliance for monitoring data at the specified interval. The data that is retrieved from the DataPower SOA appliance is written to metric log files in the format used by ITCAM for SOA. When this data is later displayed in the Tivoli Enterprise Portal, nodes are displayed in the Tivoli Enterprise Portal Navigator view that represent the DataPower SOA appliances that are being monitored. You can select workspaces under these nodes and view the services management data for the service requests flowing through the monitored DataPower SOA appliances.

The DataPower data collector can subscribe to multiple DataPower SOA appliances, and retrieve and manage data from multiple domains. This data can then be separated by DataPower domain or aggregated across multiple domains and appliances, depending on how you configure the data collector. The

DataPower data collector uses a configuration file that contains information about which DataPower SOA appliances are being monitored and information needed to establish communication with each monitored appliance.

Planning for deployment

DataPower proxies are defined within *application domains*, and DataPower users can be restricted to access some or all domains. When configuring the DataPower data collector, you must understand how the domains and users are defined on the monitored DataPower SOA appliances, to ensure that the data collector uses valid authentication credentials. This refers to user IDs and passwords that have access to the DataPower domains containing the services proxies to be monitored. In addition, you must decide how you want to aggregate or separate the data collected from those domains for display in the Tivoli Enterprise Portal.

You can use DataPower SOA appliances in several typical configurations:

Single appliance, single domain
The data collector monitors a single DataPower SOA appliance, with all of the monitored resources that are defined in a single domain on the appliance.

Single appliance, multiple domains
The data collector monitors a single DataPower SOA appliance, but that appliance has monitored resources that are defined in more than one domain on the appliance.

Multiple appliances with different configurations
The data collector monitors multiple DataPower SOA appliances, and each appliance has a different configuration of resources to be monitored. Each appliance is configured for a particular job, with no intention of load-balancing or fail-over between appliances.

Multiple appliances with identical configurations
The data collector monitors multiple DataPower SOA appliances, and all of the appliances have an identical configuration of resources being monitored. All of the appliances are configured for the same job, taking advantage of load-balancing, and fail-over capabilities between appliances.

Given these typical configurations, the DataPower data collector provides a great deal of flexibility in defining how the collected monitoring data should be separated or aggregated, across a single appliance or multiple appliances, for display in the Tivoli Enterprise Portal. The following examples illustrate how data can be separated or aggregated for managing the data from various domains and appliances:

Separation of data at the domain
You can view the services management data for the resources in a single domain, separate from the data for resources in other domains.

Aggregation of data across domains
You can view the services management data for the resources in several domains (for example, all of the domains on a DataPower SOA appliance) in an aggregated form, with no regard for the domain in which individual resources are defined.

Separation of data at the appliance

You can view the services management data for resources on a single DataPower SOA appliance, separate from the data for resources on other appliances.

Aggregation of data across appliances

You can view the services management data for the resources on several DataPower SOA appliances (for example, all of the appliances in a load-balancing *cluster*) in an aggregated form, with no regard for what activity occurs on each individual appliance.

By default, the DataPower data collector aggregates data for all of the monitored domains on a single DataPower SOA appliance (even if the domains are accessed using different credentials), and keeps the data from each DataPower SOA appliance separated. See "Enabling data collection" on page 459 for more information. However, operational flow data is collected only by individual domains. Refer to "Creating node names in Tivoli Enterprise Portal" on page 465 for additional details.

A single instance of the DataPower data collector can monitor any number of DataPower SOA appliances, limited only by the memory, CPU power, and other resources available to it.

Important: IBM supports running only a single instance of the data collector on any computer system.

Aggregation

For most ITCAM for SOA data collectors, aggregation of data is performed for each application server runtime environment. The nodes in the Tivoli Enterprise Portal Navigator view represent individual application server runtime environments that have their own individual data collectors. Because the DataPower data collector can monitor multiple DataPower SOA appliances and multiple domains within each appliance, this single application server runtime environment, single data collector model no longer applies.

Using the DataPower data collector, you assign names to groups of data, referred to as *display groups*. Each group of data is displayed as its own node in the Tivoli Enterprise Portal. Using these named display groups, you can configure the DataPower data collector to gather information from any domains on any DataPower SOA appliances for aggregation and display.

By carefully managing the way in which you name these display groups, the DataPower data collector can separate or aggregate the data in different ways, such as isolating data specific to an individual domain on a single DataPower SOA appliance, or aggregating data across several DataPower SOA appliances into a single display group. This simple display group naming mechanism gives you great flexibility in the separation and aggregation of the data that is displayed in the Tivoli Enterprise Portal. However, operational flow views are displayed by domain, not by display group. See "Creating node names in Tivoli Enterprise Portal" on page 465 for additional details.

Deployment steps

To deploy the DataPower data collector in your environment, complete the following general steps:

1. Configure your DataPower SOA appliances for monitoring (see "Configuring the DataPower SOA appliance for monitoring" for details).
2. Enable the DataPower data collector (see "Enabling data collection" on page 459 for details).
3. Run the `startDC` script to start the data collector (see "Starting and stopping the data collector" on page 474 for details), or configure the data collector to run in the background and start the background task.

Unconfiguration steps

To unconfigure the DataPower Data Collector in your environment, complete the following general steps:

1. Run the `stopDC` script to stop the Data Collector (see "Starting and stopping the data collector" on page 474 for details) when the DataPower proxy is started as a background task, or run the **`stop`**, **`quit`**, or **`exit`** command from the console to initiate an orderly shutdown of the DataPower Data Collector.
2. Disable the DataPower Data Collector (see "Disabling data collection" on page 473 for details).

Configuring the DataPower SOA appliance for monitoring

Before a DataPower SOA appliance can be monitored by the DataPower data collector, configure the DataPower SOA appliance by completing these tasks, described in more detail in the sections that follow:

- Upgrade your DataPower firmware to the minimum supported version.
- Configure a user account on the DataPower SOA appliance for use with the DataPower data collector.
- Enable the XML Management Interface on the appliance.
- Check additional optional settings for each domain to be monitored.
- Enable the ITCAM for SOA transforms for the Web Services Proxy gateways and the Multi-Protocol gateways as needed.
- Configure the AAA policy for the Web Services Proxy gateways and the Multi-Protocol gateways if you plan to monitor Web service requesters by user ID.

Upgrading the DataPower firmware version

Before using the DataPower data collector proxy, you must upgrade the firmware on DataPower SOA appliances that you want to monitor, to include the necessary monitoring and data transformation capabilities. You must upgrade the firmware to version 3.7.1 or later to use the Web Services Proxy. To use the Multi-Protocol Gateway Proxy services on your DataPower appliance, you must upgrade the firmware to version 3.7.1 Fix Pack 4 or later.

Whenever you upgrade your firmware, verify that all of your configuration settings are set correctly.

Configuring a user account on the DataPower SOA appliance

The DataPower user ID used by the data collector must belong to a user group with the following permissions:

- *Read* permission on the Login XML-Mgmt Resource Type in the default domain.
- *Read* permission on the XML-mgmt Resource Type in each domain to be monitored using this user ID.

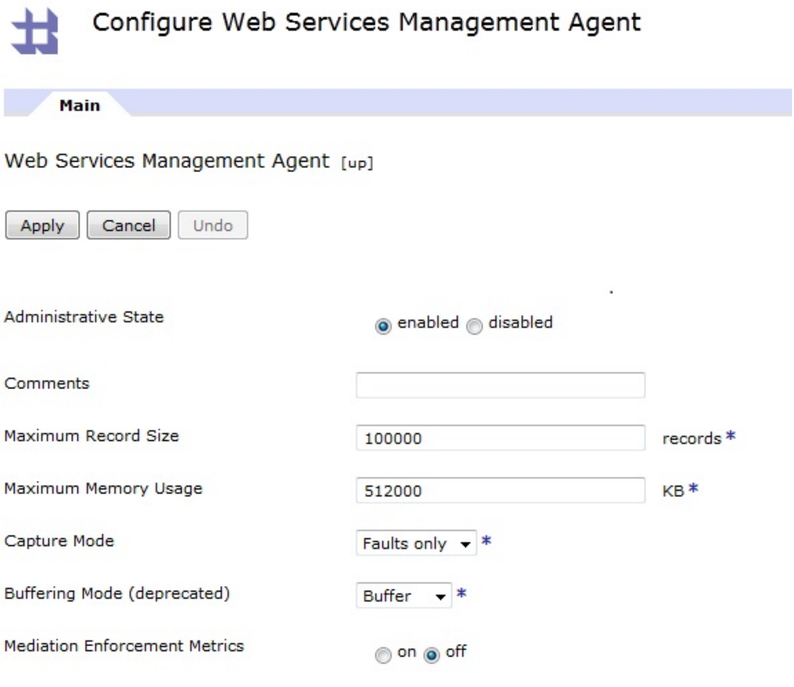
- *Read* permission on the (any) Resource Type in each domain to be monitored using this user ID.

See your *DataPower WebGUI Guide* or *DataPower CLI Reference Guide* for details on configuring user group permissions.

Configuring the XML Management Interface

The XML Management Interface on the appliance must be enabled using the DataPower administration console. To configure the XML Management interface, complete the following steps:

1. Start the DataPower administration console in a web browser (`https://hostname:9090/login.xml`).
2. Complete the following steps to enable the XML Management interface.
   a. Log in to the administration console as the admin user for the default domain.
   b. Navigate to **Objects** > **Management** > **XML Management Interface**.
   c. Make note of the port number that is displayed. You must specify this port number later when you enable or disable data collection.
   d. In the **Main** tab, find the **WS-Management Endpoint** option and select the **on** check box.
   e. Click **Apply** to activate the changes and enable the WS-Management Endpoint.
3. Complete the following steps to configure the Web Services Agent for the default domain:
   a. Navigate to **Services** > **Miscellaneous** > **Web Services Agent**. For example:


Configure Web Services Management Agent
Main
Web Services Management Agent [up]
Apply
Cancel
Undo

Administrative State	● enabled ○ disabled
Comments	
Maximum Record Size	100000 records *
Maximum Memory Usage	512000 KB *
Capture Mode	Faults only *
Buffering Mode (deprecated)	Buffer *
Mediation Enforcement Metrics	○ on ● off

Figure 63. Configure Web Services Management Agent page

   b. Set **Administrative State** to `enabled`.

c. Set the set **Buffering Mode** option to `discard` or `buffer`. The default setting is `discard`.

   When **Buffering Mode** is set to `buffer`, the Web Services Agent buffers transaction information for the current domain when no registered ITCAM for SOA data collectors are running. Buffering reduces the loss of transaction information, but consumes more memory. Transaction records are buffered until the configured size limits are reached. Buffering is a better choice when initially configuring data collection, when processing high volumes of data, or when there are multiple ITCAM for SOA subscribers.

   When **Buffering Mode** is set to `discard`, transaction information from the current domain is discarded when no registered ITCAM for SOA data collectors are running. Complications can occur if a new ITCAM for SOA subscriber replaces a former subscriber. High volumes of transactions might cause the Complete Records Count to reach the configured Maximum Record Size limit and transaction information to be discarded. Setting **Buffering Mode** to `discard` is suited to an environment where there is a single ITCAM for SOA subscriber, where the DataPower appliance is handling a low volume of transaction data, and where the ITCAM for SOA subscriber is collecting a low volume of metrics. For information about troubleshooting scenarios where transaction metrics are being discarded, see the *IBM Tivoli Composite Application Manager Troubleshooting Guide*.

d. Adjust the values for **Maximum Record Size** and **Maximum Memory Usage**, if necessary.

e. If you want the data collector to record message content in addition to summary metrics, change **Capture Mode** from `faults` to `all-messages`.

4. Configure the Web Services Agent for *all other domains* that are monitored by the DataPower data collector. For each domain, switch to the domain and complete step 3a on page 446 to step 3e.

Configuring DataPower Processing Rules

In addition to upgrading your DataPower firmware, you might have to add XSL transforms to the action rules in each processing rule for each affected Web Services Proxy or Multi-Protocol Gateway Proxy object:

- If you are monitoring a WS-Proxy without topology support or transaction tracking API (TTAPI) support, no transforms are necessary.
- If you are monitoring topology or you configured a TTAPI in a WS-Proxy, the preloaded transforms must be added to your processing rules.
- If you are monitoring a Multi-Protocol gateway, certain transforms must be created.
- If you are monitoring topology or you configured a TTAPI on a Multi-Protocol gateway, more logic must be added either to those transforms or into additional transforms.

This section describes the procedures for configuring DataPower processing rules for Web Services Proxy gateways and DataPower Multi-Protocol gateways.

Configuring processing rules for DataPower Web Services Proxy gateways

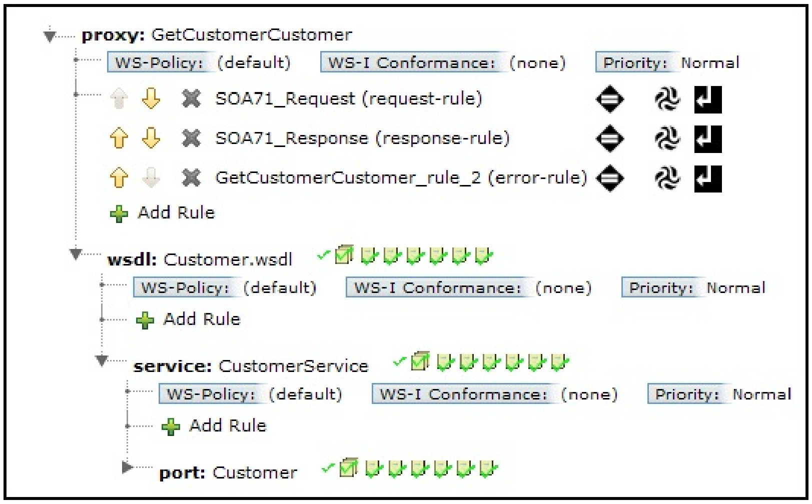
This section describes the procedures for configuring DataPower processing rules for Web Services Proxy gateways.

For each Web Services Proxy object, you need to add these transforms, which are included in your DataPower firmware:

- soapreq.xsl
- soaprsp.xsl
- soaperror.xsl

Generally, the procedure to add these XSL transforms to the request and response paths involves these steps:

1. Open the Web Services Proxy Object.
2. Select the **Policy** tab.



proxy: GetCustomerCustomer
WS-Policy: (default) WS-I Conformance: (none) Priority: Normal
SOA71_Request (request-rule)
SOA71_Response (response-rule)
GetCustomerCustomer_rule_2 (error-rule)
Add Rule
wsdl: Customer.wsdl
WS-Policy: (default) WS-I Conformance: (none) Priority: Normal
Add Rule
service: CustomerService
WS-Policy: (default) WS-I Conformance: (none) Priority: Normal
Add Rule
port: Customer

Figure 64. Enabling ITCAM for SOA transforms in DataPower

3. If you currently do not have a processing rule defined, expand the node tree to display subnodes (**proxy**, **wsdl**, **service**, and others).
4. Select an **Add Rule** icon and continue to configure this new rule as if it already exists.
5. For an existing or newly added rule, complete the following steps:
   a. Add a **Match** action to the rule (the equal sign (=) icon), as needed, to match all messages, or to only match those you intend to monitor.
   b. Add a **Transform** action (the three-prong swirl icon) to add the ITCAM for SOA transforms that are preloaded in the firmware.
      - For a Request rule, use the `store:///soapreq.xsl` transform.
      - For a Response rule, use the `store:///soaprsp.xsl` transform.
      - For an Error rule, use the `store:///soaperror.xsl` transform.

      Important: For an Error rule, your **Match** action must match errors, not normal responses. This is an option when you configure your Match.
   c. Add a **Results** action to the rule (the arrow icon) to return the transformed message.
6. Apply and save your changes.

You can provide your own XSL style sheets to implement further configuration changes. Refer to the WebSphere DataPower documentation for more information about processing rules.

To use the requester identity monitoring function that is provided with ITCAM for SOA, you must complete one of the following configuration tasks:

- Configure an AAA policy for the WSP that you intend to monitor (see "Configuring the AAA policy" on page 458).
- Customize the requester identity using an XSL stylesheet (see "Configuring processing rules for DataPower gateways to monitor by requester identity" on page 457).

Configuring processing rules for DataPower Multi-Protocol Gateways

A DataPower multi-protocol gateway service handles SOA messages in a variety of transport protocols and message formats. It can process almost any incoming message and transform the message into a completely different format, if needed, before forwarding it to a server to perform additional business processing.

For example, you might use a multi-protocol gateway to provide an HTTP front end that receives a SOAP message, transforms it into a proprietary XML format, and places it on a queue for the Message Queue transport protocol. Unlike a Web Service Proxy, a multi-protocol gateway is not restricted to processing messages that are described by Web Services Description Language documents.

Because of its flexibility and its independence from Web Services Description Language document restrictions, configuring a multi-protocol gateway is different from configuring a web service proxy. The web service proxy knows the service port name and namespace, and the operation name and namespace of a SOAP message from information in the Web Services Description Language documents.

The multi-protocol gateway, however, cannot recognize this information because it has no Web Services Description Language documents. Therefore, it cannot pass this information along to the ITCAM for SOA data collector.

Instead, you must provide this information about service port name, service port namespace, operation name, and operation namespace, by writing the necessary logic into an XSLT processing rule in your DataPower multi-protocol gateway.

To record transaction data in the web service management (WSM) agent of each domain, your application developers must add additional logic to the XSLT processing rules. The ITCAM for SOA data collector polls the WSM agent at regular intervals to collect the data from the WSM agent.

For transactions to appear in ITCAM for SOA operational flow topology views, the application developers must write additional logic into the XSLT processing rules to track relationships among related web services.

The additional logic in your processing rules must perform the following steps:

1. Identify the message by setting message attributes.
2. Calculate the correlator for each request and response message in the transaction.
3. Record data about the request and response messages in the WSM agent at the end of each transaction.

Identifying the message: The `wsm-agent-append()` function sends data about the transaction to the WSM agent, from where the data is polled by ITCAM for SOA.

Before you invoke the `wsm-agent-append()` function, you must construct a processing variable containing a `dpwsm:wsa-record` nodeset and provide it as an argument to this method. This nodeset contains the various attributes that describe the message and the transaction.

Most of the elements in this nodeset can be set to their default values from the processing context. However, due to the absence of Web Services Description Language, the following elements must be set explicitly in your XSL:

ws-operation
The fully qualified operation namespace and operation name (for example, `{www.opnamespace.com}myOperation`).

service-port
The fully qualified service port namespace and service port name (for example, `{www.spnamespace.com}myServicePort`).

is-one-way
Set to `true()` if this operation is one-way, or `false()` if this operation is two-way.

webservice
Specifies one of the following numerical values that identify the format of the message being processed:

- The value `8` refers to a SOAP message.
- The values `9` refers to an XML message.
- The value `10` refers to a non-XML or binary message.

You should not set explicit values for any of the following elements, because they are calculated automatically by various processing tasks:

- ws-correlator-sfid
- ws-client-socode
- ws-dp-socode
- ws-server-socode
- ws-client-hopcount
- ws-server-hopcount
- start-time
- duration-ms
- front-latency-ms
- back-latency-ms
- request-size
- response-size

For more information about out the contents of this nodeset, see the `dp:wsm-agent-append()` function in the *Metadata extension functions* section of the DataPower Extensions Elements and Functions Catalog for the appliance. For a sample style sheet, see "Using sample style sheets to create transform actions" on page 454.

Tracking relationships between web services using a correlator: For transactions to appear in ITCAM for SOA operational flow topology views, you must add additional logic to your processing rules to track relationships among related web services.

When the ITCAM for SOA data collector monitors a Web Service Proxy, the correlator is handled by the `soapreq.xsl` and `soaprsp.xsl` style sheets that are provided with the appliance firmware. When you use ITCAM for SOA to monitor multi-protocol gateways, however, you must invoke the logic necessary to calculate and propagate the correlator.

The logic extracts a string, calls a `dp:exter-correlator()` function, and attaches the result to the message. The `exter-correlator()` function uses a propriety algorithm to calculate and propagate the correlator in transactions. Using this correlator, each of several concurrent messages are tracked independently and accurately, without errors from the heuristic algorithm.

Handing the correlator in request messages: When the gateway receives a request message from the client, it processes this message, and forwards it to the server for additional processing. Figure 65 displays the logic that must be added to the request processing logic to handle the correlator.

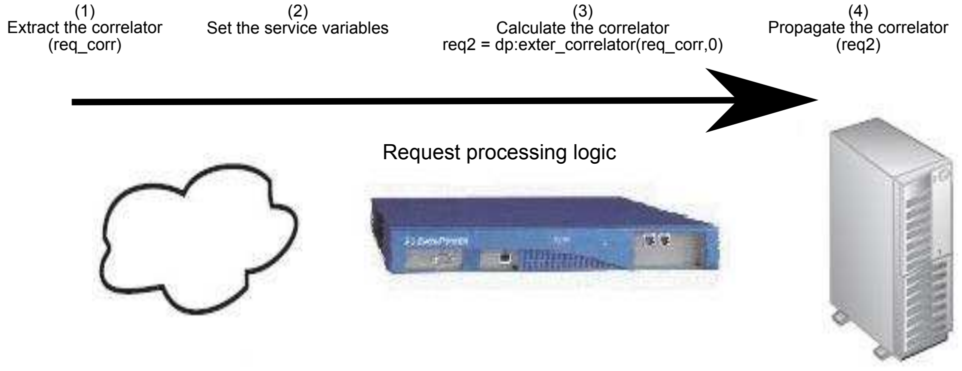


Figure 65. Logic added to the request processing logic to handle the correlator

To correlate the transition of a request message through a multi-protocol gateway, add logic to the processing rules to complete these steps:

1. Extract the incoming correlator.
   If your multi-protocol gateway receives SOAP messages from a web application server that is monitored by ITCAM for SOA, then you should include logic to receive an attached correlator string, if one is available.

   The ITCAM for SOA data collector on the sending server adds a standard SOAP header named `{http://www.ibm.com/KD4Soap}KD4SoapHeaderV2` to each message that is sent. Your XSL logic must check for the presence of this header, and if it is present, extract the text node from within this element, similar to the following example:

   ```
   <xsl:choose xmlns:kd4="http://www.ibm.com/KD4Soap">
       <xsl:when test=".//kd4:KD4SoapHeaderV2">
          <xsl:value-of select=".//kd4:KD4SoapHeaderV2"/>
       </xsl:when>
       <xsl:otherwise>
          <xsl:text>NEW_CORRELATOR</xsl:text>
       </xsl:otherwise>
   </xsl:choose>
   ```

2. Set the following service variables to identify the message:

   var://service/wsm/operation
      The fully qualified operation namespace and operation name (for example, `{www.opNamespace.com}myOperation`).

var://service/wsm/service-port
The fully qualified service port namespace and service port name (for example, `{www.spNamespace.com}myServicePort`).

var://service/soap-oneway-mep
Set to `true()` if this operation is one-way, or `false()` otherwise.

var://service/wsm/service
Specifies one of the following numerical values that identify the format of the message being processed:

- The value `8` refers to a SOAP message.
- The values `9` refers to an XML message.
- The value `10` refers to a non-XML or binary message.

When you set these variables, allow the `ws-operation`, `service-port`, `webservice`, and `is-one-way` elements of the `wsa-record` nodeset to take their default values.

3. Calculate the correlator.

   Invoke the `dp:exter-correlator()` function. The first argument is the incoming correlator string. If you do not have an incoming correlator, use the literal string `NEW_CORRELATOR` instead. For a request message, specify `0` for the second argument.

4. Propagate the correlator.
   The return value from the `dp:exter-correlator()` function is the new correlator. Attach this string to the data collectors on the back-end servers.

   If you are sending SOAP messages, add XSTL logic to construct a `{http://www.ibm.com/KD4Soap}KD4SoapHeaderV2` header and add it to the SOAP Header section of the outbound message.

For sample style sheets, see "Using sample style sheets to create transform actions" on page 454.

Handling the correlator in a response message: When the gateway receives a response message from the server, it processes that message as needed, and forwards that response back to the client. Figure 66 displays the logic that must be added to the response processing logic to handle the correlator.

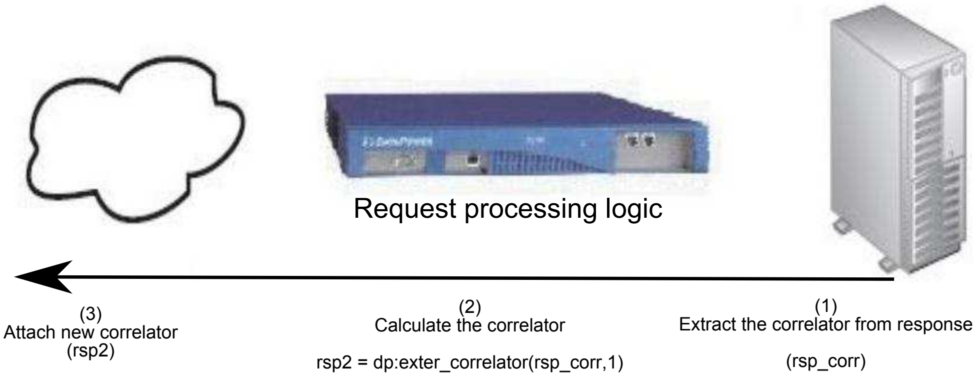


Figure 66. Logic added to the response processing logic to handle the correlator

The process of calculating the correlator for a response message is similar to that of a request message. When processing a response message, add the following logic necessary to calculate and propagate the correlator:

1. Extract an incoming correlator, if one is present.

2. Calculate a new correlator.
   Pass in the newly extracted correlator, but use 1 instead of 0 for the second argument.
3. Attach the newly calculated correlator.

For a sample style sheets, see "Using sample style sheets to create transform actions" on page 454.

Handling the correlator in an error response: The process of calculating the correlator for an error message is similar to that of a response message.

For an error processing rule, be careful to identify whether the error is on a request or a response, setting the direction according to the var://service/response-mode variable, as shown in the following example code:

```
{noformat}
<!-- Determine whether the error is on a request or response -->
<xsl:variable name="rmode">
<xsl:value-of select="dp:variable('var://service/response-mode')"/>
</xsl:variable>

<!-- Calculate the new correlator -->
<xsl:variable name="newCorrelator">
<xsl:choose>
<xsl:when test="$rmode='2'">
<xsl:value-of select="dp:exter-correlator($InboundCorrelator,'1')"/>
</xsl:when>
<xsl:otherwise>
<xsl:value-of select="dp:exter-correlator($InboundCorrelator,'0')"/>
</xsl:otherwise>
</xsl:choose>
</xsl:variable>
<dp:set-variable name="'var://context/kd4/responseCorrelatorOut'"
value="$newCorrelator"/>
{noformat}
```

The processing-rule context automatically populates the error details, and the response is identified as a fault to ITCAM for SOA. You must include the same XSTL logic on an error rule that you include on a response rule.

For more information about using dp:exter-correlator() function and for code examples, see the *Metadata extension functions* section of the DataPower Extensions Elements and Functions Catalog for the appliance. For a sample style sheet, see "Using sample style sheets to create transform actions" on page 454.

Recording transaction data on the appliance: The wsm-agent-append() function records the various attributes of this transaction in the WSM agent. The data is available for ITCAM for SOA to collect.

Your processing rules must call the wsm-agent-append() function as close as possible to the end of the response processing rules and error processing rules.

Remember: You must call the exter-correlator() before you call the wsm-agent-append() function.

For more information about using the wsm-agent-append() function and for code examples, see the *Metadata extension functions* section of the DataPower Extensions Elements and Functions Catalog for the appliance. For a sample style sheet, see "Using sample style sheets to create transform actions" on page 454.

Using sample style sheets to create transform actions: A sample set of style sheets is provided in `SampleStyleSheets.zip` on the ITCAM for SOA Service Management Connect wiki page. The style sheets are provided to assist in creating transform actions. See the wiki page for any restrictions that might apply to using the sample style sheets.

Figure 67 shows the XSLT logic that must be added to the processing rules to correlate messages across transaction data from multi-protocol gateways and to record the transaction data it the WSM agent for collection by ITCAM for SOA.

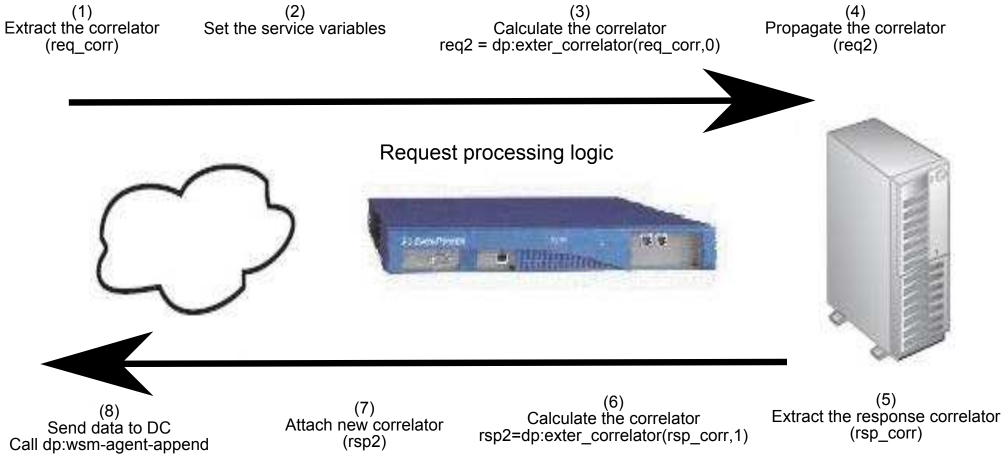


Figure 67. Adding additional logic to track messages

Use the sample style sheets to create and add logic to the request, response, and error messages to perform the following actions:

1. Extract the request correlator, if present.
   Use the style sheet `ExtractRequestCorrelator.xsl` as an example.
2. Set the service variables, if you plan to create a correlator to track request and response messages.
   Use the style sheet `SetMessageAttributes.xsl` as an example.

   Important:
   - The `wsa-record` nodeset should take the default values from the service variables.
   - You must edit the `SetMessageAttributes.xsl` file to use the service and operation names that are appropriate for your application.
3. Calculate the correlator for the request message.
   Use the style sheet `CalculateRequestCorrelator.xsl` as an example.
4. Propagate the correlator to the server.
   Use the style sheet `AttachRequestCorrelator.xsl` as an example.
5. Extract the correlator from the response message.
   Use the style sheet `ExtractResponseCorrelator.xsl` as an example.
6. Calculate the correlator for the response message.
   Use the style sheet `CalculateResponseCorrelator.xsl` as an example.
7. Attach the new correlator to the response message.
   Use the style sheet `AttachResponseCorrelator.xsl` as an example.
8. Record transaction data in the web services management agent of the domain.
   Use the style sheet `SubmitMonitoringData.xsl` as an example.

Important: If you are integrating with a DataPower appliance version 6.0 and you enabled the option **Monitor via Web Services Management Agent** for Multi-Protocol Gateways on the Proxy settings tab of the appliance, you no longer require the `SubmitMonitoringData.xsl` style sheet.

To use the requester identity monitoring function that is provided with ITCAM for SOA, you must complete one of the following configuration tasks:

- Configure an AAA policy on each gateway that you intend to monitor
- Customize the requester identity using an XSL style sheet. You specify the requester identity using the `SubmitMonitoringData.xsl` style sheet in step 8 on page 454.

For more information about tracking the requester identity, see "Configuring processing rules for DataPower gateways to monitor by requester identity" on page 457.

Enabling DataPower Multi-Protocol Gateways transforms: This section describes the procedures for adding the XSL transforms that you created for multi-protocol gateways (see "Using sample style sheets to create transform actions" on page 454) to the request, response, and error processing rules.

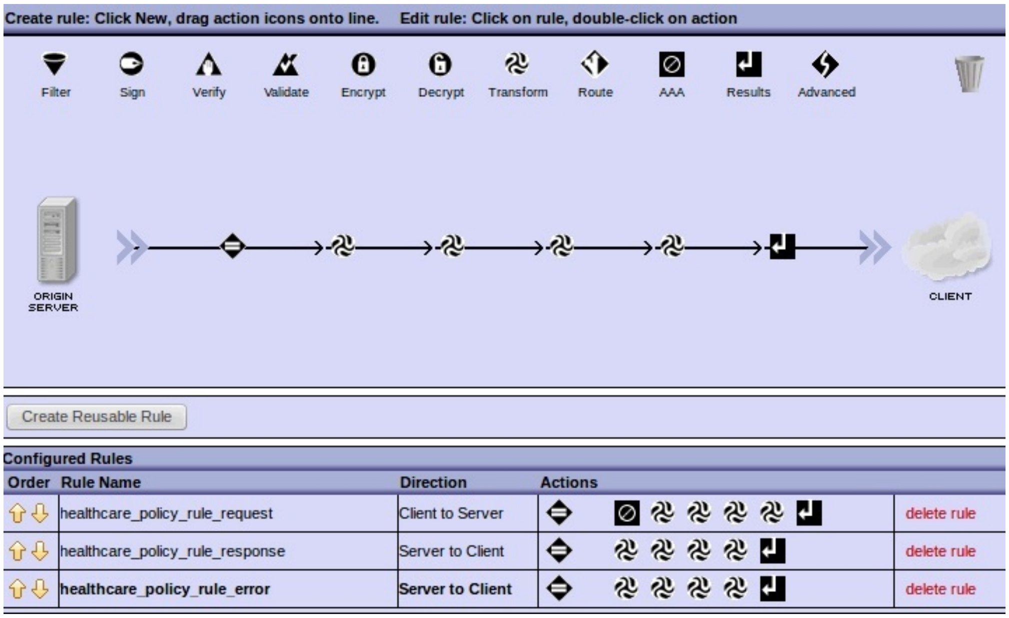
To add the XSL transforms to the request, response, and error paths, complete the following steps:

1. Open the multi-protocol gateway object.
2. Select a policy from the **Multi-Protocol Gateway Policy** drop-down list and click the edit button.
3. For the request processing rule, add the style sheets that you created to perform the following actions:
   a. Extract the request correlator.
   b. Set the service variables.
   c. Calculate the correlator for the request message.
   d. Propagate the correlator to the server.

   Click the transform actions (the three-prong swirl icon) button to add each style sheet.

   For more information about the sample style sheets to use to create each transform, see "Using sample style sheets to create transform actions" on page 454.
4. For the response and the error processing rules, add the style sheets that you created to complete the following actions:
   a. Extract the correlator from the response message.
   b. Calculate the correlator for the response message.
   c. Attach the new correlator to the response message.
   d. Record the transaction data in the WSM agent of the domain for collection by ITCAM for SOA.

   For more information about the sample style sheets to use to create each transform, see "Using sample style sheets to create transform actions" on page 454.
5. Verify that you created three processing rules (request, response, and error processing rules) and that you added a match action (the equal sign (=) icon), the four transform actions (the three-prong swirl icon), and a results action (the arrow icon) to each rule. For example:



Configured Rules

Order	Rule Name	Direction	Actions	
⇧ ⇩	healthcare_policy_rule_request	Client to Server	◆ ⊘ ✲ ✲ ✲ ✲ ↵	delete rule
⇧ ⇩	healthcare_policy_rule_response	Server to Client	◆ ✲ ✲ ✲ ✲ ↵	delete rule
⇧ ⇩	**healthcare_policy_rule_error**	**Server to Client**	◆ ✲ ✲ ✲ ✲ ↵	delete rule

Figure 68. Processing rules for the request, response, and error paths

6. Apply and save your changes.

Additional considerations: Consider the following requirements, limitations, and troubleshooting tips when configuring processing rules:

Service Port Name Type:
Because of known limitations, the Service Port Name Type attribute `SPNAMETYPE` is always set to 1 (WSDL Port Name), regardless of the values that are used in the `var://service/wsm/service` variable and the `webservice` element. Accurate values are necessary for correct calculation of various other identifiers within the context, however, so be sure to set them accurately.

Logging return codes:
Log the return code from `dp:wsm-agent-append()`. If there is an error in this function, or a problem with the set of data you collected for it to log, the return value from this function describes the error. To debug problems with this function, your XSL logic must make this return value available. If your return value says `error - no record`, this does not reflect an error in your XSL; it indicates that there are no subscriptions active for this domain at the moment. You can activate the ITCAM for SOA data collector or set the buffer mode setting for this domain to buffer to save metric records when the DataPower data collector is not running.

XSL variables and syntax:
Pay careful attention to references to XSL variables and DataPower context variables, and to use single quotation marks, and double quotation marks, correctly as needed.

Troubleshooting:
Other troubleshooting tools and techniques, including using a multistep probe and referring to the log files on both the DataPower appliance and on the ITCAM for SOA data collector, still useful in troubleshooting issues with monitoring the multi-protocol gateway service.

Configuring processing rules for DataPower gateways to monitor by requester identity

Before you use the requester identity monitoring function that is provided with ITCAM for SOA, you must configure the Web Services Proxy Gateway or the Multi-Protocol Gateway to track the requester identity using one of the following options:

- Configure an AAA policy on each gateway that you intend to monitor (see “Configuring the AAA policy” on page 458).
- Create an XSL style sheet to define a value for `ws-client-id` and add it after each response and error processing rule that you want to monitor (see “Customizing the requester identity”).

ITCAM for SOA can only return client ID requester identity information for the message when the gateway is configured to track requester identities.

The feature to perform service monitoring by requester identity in ITCAM for SOA is disabled by default. To enable service monitoring by requester identity, use the available Tivoli Enterprise Portal Take Action commands AddRequesterIdentity_610 and EnableReqIDMntr_610, and others, as described in the *IBM Tivoli Composite Application Manager for SOA User's Guide*.

Important: Fault monitoring by requester identity is always enabled for the DataPower data collector. For information about configuring the requester identity type for fault monitoring, see “Configuring the requester identity type for fault monitoring” on page 479.

Customizing the requester identity: You can define a value for Requester ID by customizing the DataPower variable `ws-client-id` using an XSL style sheet.

Sample style sheets are available from the ITCAM for SOA Service Management Connect wiki page.

To customize the requester identity, use the `SubmitMonitoringData.xls` style sheet for a Multi-Protocol Gateway and the `CustomiseMonitoringData.xls` style sheet for a Web Services Proxy Gateway.

In the style sheet, the following lines of code are used to determine the requester identity:

```
<dpwsm:ws-client-id default="yes" /> - <!-- Default uses internal
calculation -->
<dpwsm:ws-clientid-extmthd default="yes" /> - <!-- Default uses
internal calculation -->
```

Replace these lines in the style sheet with lines similar to the following lines:

```
<xsl:variable name="customName" select="dp:encode('ws-client-id','base-64')"/>
 <dpwsm:ws-client-id><xsl:value-of select="$customName"/></dpwsm:ws-client-id>
 <dpwsm:ws-clientid-extmthd>custom</dpwsm:ws-clientid-extmthd>
```

The first argument of `dp:encode()` is the value that you want to supply for the requester identify, for example, `dp:encode('`*`my_requester_identity`*`','base-64')`.

For both Multi-Protocol Gateways and Web Services Proxy Gateway, apply the style sheet to the response and error processing rules.

Configuring the AAA policy

If you plan to use the requester identity monitoring function that is provided with ITCAM for SOA to monitor by user identity, you can configure an AAA policy for the Web Services Proxy Gateway and Multi-Protocol Gateway on each processing rule that you intend to monitor.

If you currently have an AAA policy in place, no changes to that policy are required.

If no AAA policy exists on the processing rule, you can open a DataPower administrative console to add and configure the AAA policy. Refer to the procedures documented in Chapter 30 of the *IBM WebSphere DataPower XML Security Gateway XS40 WebGUI Guide*, version 3.7.3, for more information.

Important: Configure the processing rules to verify the AAA policy at the start of the processing rule before you extract the incoming correlator.

Extraction methods and priorities: Like most SOA environments, there are many ways to configure an AAA policy, and many different types of credentials are available. ITCAM for SOA selects the first available identity type from the prioritized list in Table 57.

Table 57. Extraction methods and priorities used by the DataPower DC to obtain the user identity.

Client ID extraction method	Client ID type	Priority
http-basic-auth	User name	1
LTPA-auth	User ID	2
Saml-attr-name	User name	3
Saml-authen-name	User name	4
Wssec-username	User name	5
Custom	Result of XSL process	6
Client-IP-address	IP address	7
Client-ssl	Dn	8
Signer-dn	Dn	9
Wssec-binary-token	Token	10
Ws-secure-conversation	Context	11
Kerberos	Token	12
LTPA-token	Token	13
Ws-trust	Token	14
Cookie-token	Token	15
Xpath	Token	16
Saml-artifact	Artifact	17

All of the supported extraction methods are listed in the first column. The extraction methods are prioritized by the following rules:

- Sort the extraction methods by the precision of the corresponding user identity, from most specific to least specific:

```
Username –> IP address –> Dn –> Token
```

- Within the extraction methods that extract the user name and user ID, system-level authentication takes priority over message-level authentication:

  ```
  (http-basic-auth, LTPA-auth, Saml-attr-name, Saml-authen-name)
   –> (Wssec-username)
  ```

These priorities are only considered when multiple extraction methods are configured in the AAA policy. You cannot adjust these priorities.

Enabling data collection

This section describes how to configure the DataPower environment for data collection.

The DataPower configuration file

For the DataPower data collector, the Data Collector Configuration utility and the **KD4configDC** command manipulate the contents of a special DataPower configuration file by adding sections to the file when new DataPower monitoring is enabled, and removing sections from the file when monitoring is disabled. Each invocation of the Data Collector Configuration utility or the **KD4configDC** command adds, updates, or removes one section of the DataPower configuration file. Each section of the DataPower configuration file might be associated with its own data group, or it might be part of a larger data group to which other sections of the configuration file also belong.

The DataPower data collector uses this configuration file to identify the DataPower SOA appliances that are to be monitored and to specify all of the information that is needed to communicate with those appliances. Typical information that is stored for each connection includes host name and port, user ID and password, domains to monitor, and polling interval.

The configuration file is in the *ITCAM4SOA_Home*/KD4/config directory on Linux or UNIX systems and the *ITCAM4SOA_Home*/KD4/config directory on Windows systems and is called KD4.dpdcConfig.properties. This file is maintained separately from the existing KD4.dc.properties configuration file. This is a sample DataPower configuration file:

```
# Sample DataPower data collector configuration file
DataPower.count=3
#
DataPower.host.1=dpbox1
DataPower.port.1=5550
DataPower.path.1=/
DataPower.poll.1=60
DataPower.user.1=admin
DataPower.encpswd.1=#$%*&
DataPower.domainlist.1=default,testdom1
DataPower.displaygroup.1=dpbox1
DataPower.subExpire.1=15
DataPower.maxrecords.1=1000

#
DataPower.host.2=dpbox2
DataPower.port.2=5550
DataPower.path.2=/
DataPower.poll.2=30
DataPower.user.2=user1
DataPower.encpswd.2=&*%$#
DataPower.domainlist.2=userdom1,userdom2,userdom3
DataPower.displaygroup.2=user_doms
DataPower.subExpire.2=15
```

```
DataPower.maxrecords.2=1000
#
DataPower.host.3=dpbox2
DataPower.port.3=5550
DataPower.path.3=/
DataPower.poll.3=30
DataPower.user.3=admin
DataPower.encpswd.3=*%$#&
DataPower.displaygroup.3=all_doms
DataPower.subExpire.3=15
DataPower.maxrecords.3=1000
```

In the example, there are three sections in the configuration file. The properties in each of the three sections provide all of the information that is needed to establish and manage a single connection or session with each DataPower SOA appliance.

Change the information in this configuration file using either the Data Collector Configuration utility or the **KD4configDC** command. You can only modify the parameters that are set when you first run the Data Collector Configuration utility or when you first issued the **KD4configDC** command. To set additional parameters, you must manually add them to the configuration file.

Using various combinations of parameters in the Data Collector Configuration utility input pages or in the **KD4configDC** command, you can achieve different monitoring configurations to separate or aggregate data among domains and appliances. See "Considerations for enabling data collection for DataPower monitoring" on page 468 for more information.

Before you configure your DataPower environment for data collection, consult with your local systems management planners to understand which domains on which DataPower SOA appliances are to be monitored and how the data from these domains and appliances should be separated or aggregated for display in the Tivoli Enterprise Portal.

To set the `DataPower.maxrecords` property to an optimal value, it is useful to determine the number of transactions that are processed by each of the configured domains. The `DataPower.maxrecords` property must be set in line with the expected traffic levels of each configured domain. For more information about setting the transaction rate, see "Optimizing performance" on page 481.

Restriction: In an upgrade scenario, to set the maximum number of records for an existing display group, you must add the `DataPower.maxrecords` parameter manually to the section in the `KD4.dpdcConfig.properties` file that configures the display group.

Additional properties

Beginning with ITCAM for SOA version 7.2 Fix Pack 1, you can optionally add the following properties manually to the `KD4.dpdcConfig.properties` file:

DataPower.dimension.domain

Adds the DataPower domain attribute to the Service Inventory_610, the Service Inventory Requester Identity_610, and the Fault Log_610 tables. The domain attribute is added to the Application Server Cluster Name column in each table.

Because the Application Server Cluster Name is a dimensional field within the ITCAM for SOA Reports schema, when you run reports on the Tivoli Data Warehouse, you can display aggregated metric data by domains.

If the `DataPower.domainlist` parameter contains more than one domain, the `DataPower.dimension.domain` parameter is treated as being set to false.

DataPower.alias
Assigns an alias to the DataPower host. If this property is set, the alias is added to the Application Server Cell Name column in the Service Inventory_610, the Service Inventory Requester Identity_610, and the Fault Log_610 tables. Alternatively, you can use the `DataPower.displaygroup` property to create an alias for the DataPower host.

DataPower.multihost.group
The `DataPower.displaygroup` property defines the name to display for the DataPower appliance node in the Navigator view in the Tivoli Enterprise Portal. When the property is set, data from all DataPower appliances that are associated with the display group is aggregated. The data is available from the single node in the Navigator view.

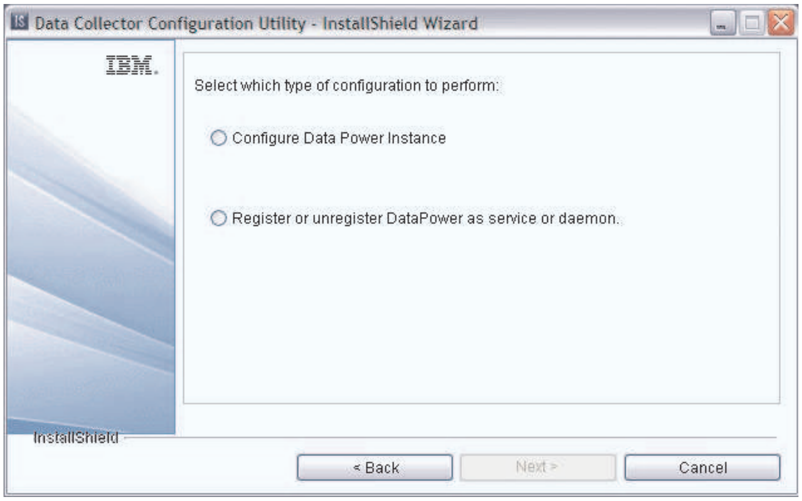
The display group might be associated with different domains on the single DataPower appliance. In the Service Inventory_610, the Service Inventory Requester Identity_610, and the Fault Log_610 tables, the Application Server Node Name attribute displays the name of this appliance. Alternatively, the display group might be associated with multiple appliances. The Application Server Node Name attribute displays the name of only one of the appliances.

By setting the `DataPower.multihost.group` property to `true`, you indicate that there are multiple appliances associated with a display group. The Application Server Node Name attribute is not populated. By setting the property to `false`, you indicate that the display group is associated with a single DataPower appliance. The name of the DataPower appliance is added to the Application Server Node Name column. If the `DataPower.multihost.group` property is not specified in the configuration file, the property is set to `false`.

Enabling data collection using the Data Collector Configuration utility

To enable data collection using the Data Collector Configuration utility, complete the following steps:

1. Run the Data Collector Configuration utility (see “Running the Data Collector Configuration utility” on page 378):
   a. Select the DataPower SOA Appliance runtime environment.
   b. Select the **Configure** > **DataPower Instance** option.



Data Collector Configuration Utility - InstallShield Wizard

Select which type of configuration to perform:

○ Configure Data Power Instance

○ Register or unregister DataPower as service or daemon.

Figure 69. Enabling data collection on a Data Power instance

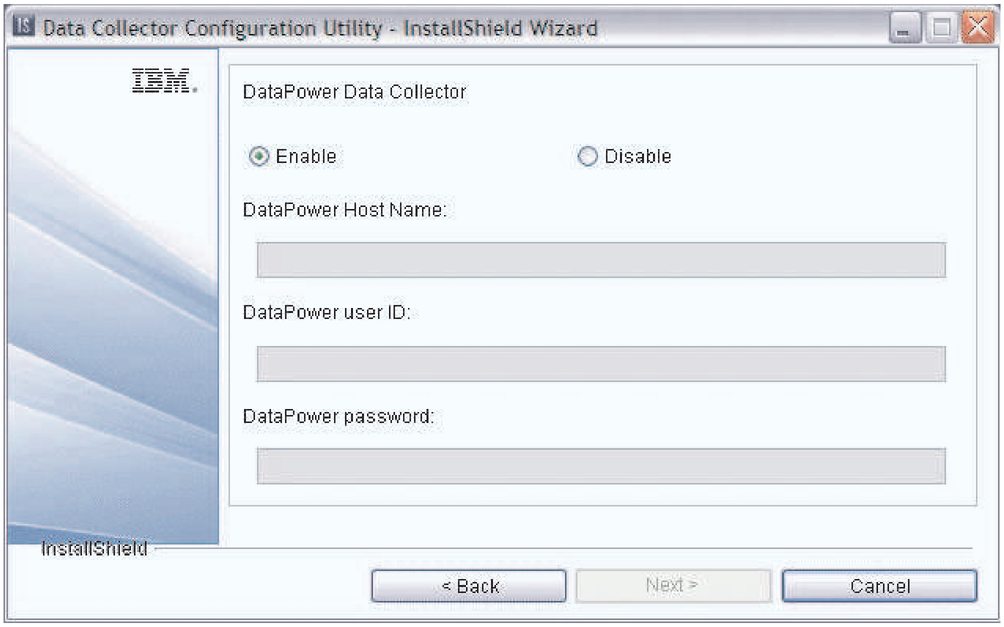
c. Select the option to enable data collection.

   For the remaining input parameters, refer to Table 58 on page 464 for a description of the information that is required, and see the additional information and examples of running the **KD4configDC** command to learn more about how to specify these parameters for your environment.

d. Specify the DataPower Host Name.

e. Specify the DataPower user ID.

f. Specify the DataPower password.



Data Collector Configuration Utility - InstallShield Wizard

DataPower Data Collector

● Enable ○ Disable

DataPower Host Name:

DataPower user ID:

DataPower password:

Figure 70. Enabling data collection in a DataPower runtime environment

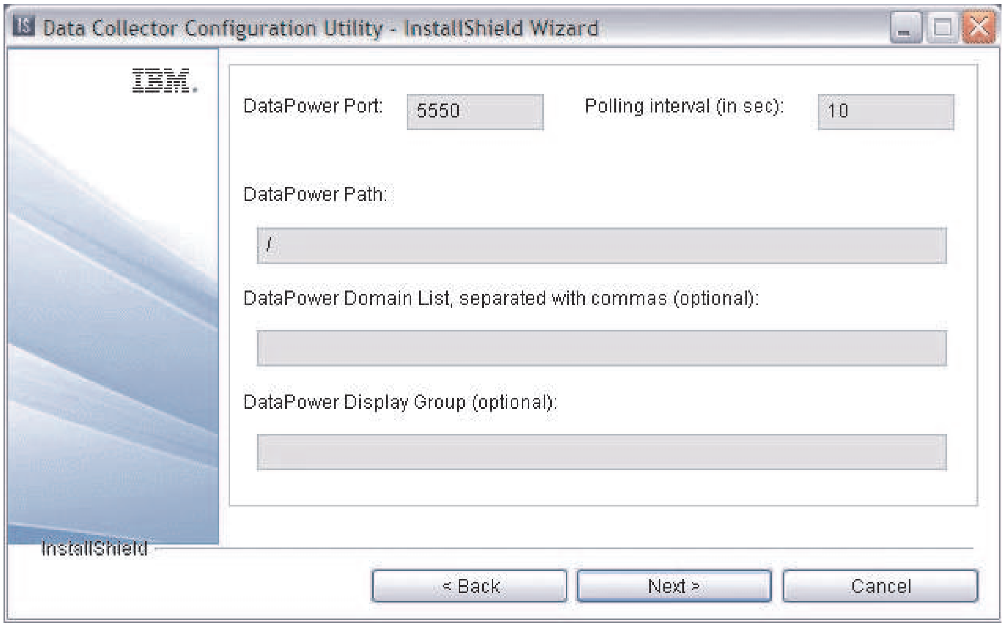
g. The default DataPower port number (5500) and the default polling interval (10 seconds) are provided. Accept these defaults or specify different values.

h. Verify that the DataPower Path is set to /.

Restriction: You cannot specify a path other than /. Changing its value has no effect.

i. Specify the DataPower Domain List.

j. Optionally specify the DataPower Display Group.



DataPower Port: 5550

Polling interval (in sec): 10

DataPower Path: /

DataPower Domain List, separated with commas (optional):

DataPower Display Group (optional):

Figure 71. Enabling data collection in a DataPower runtime environment

k. Wait for the configuration utility to complete the operation.

l. Exit the utility.

Important: When you deploy the DataPower data collector, you must start the data collector once you have enabled it to begin collecting data. For more information about starting the data collector, see “Starting and stopping the data collector” on page 474.

Enabling data collection using the KD4configDC command

The syntax for running the **KD4configDC** command for the DataPower environment is similar to the syntax for other supported ITCAM for SOA data collector environments. To run the **KD4configDC** command, first navigate to the following location, depending on your operating system:

Enter the **KD4configDC** command:

- For supported Windows operating systems:

```
KD4configDC {-enable | -disable} -env 8 <env specific parameters>
```

- For supported AIX, Solaris, HP-UX, and Linux operating systems:

```
KD4configDC.sh {-enable | -disable} -env 8 <env specific parameters>
```

Specifying KD4configDC parameters

The `env specific parameters` defined for the DataPower invocation of the **KD4configDC** command are a series of key and value pairs that define the necessary properties for the affected section of the DataPower configuration file. These key and value pairs, which you can specify in any order on the command line, are shown in Table 58 on page 464.

Table 58. DataPower key and value pairs for the KD4configDC command

Parameter	Optional / Required	Default value	Description
–host *host name or IP address*	Required		Defines the DataPower SOA appliance host name or IP address. This host name is used to establish a socket connection and is used as part of the Web address pointing to the DataPower SOA appliance. This value can be any length string, with no blank characters. See "Creating node names in Tivoli Enterprise Portal" on page 465 regarding possible truncation of this value in the node name.
–user *user ID*	Required		Defines the DataPower SOA appliance authentication user. This user must be a valid user for the DataPower SOA appliance defined by the `-host` parameter. See your DataPower documentation for information about creating and managing user IDs for DataPower SOA appliances. See "Configuring a user account on the DataPower SOA appliance" on page 445 for more information.
–pswd *password*	Optional	User is prompted, if necessary	Defines the DataPower SOA appliance authentication password, entered in clear text (not encoded). This password must be valid for the user defined in the `–user` parameter, and must be valid for the DataPower SOA appliance defined by the `–host` parameter. This password is automatically converted to an encoded (masked) form and is stored in the DataPower configuration file. See your DataPower documentation for information about creating and managing passwords for DataPower SOA appliances.
–port *port number*	Optional	5550	Defines the DataPower SOA appliance port number. This port number is used to establish a socket connection and is used as part of the Web address pointing to the DataPower SOA appliance. This value must be an integer from 0 to 65535. If this parameter is not specified, the default value is used.
–path *path string*	Required	/	Defines the DataPower SOA appliance path. This path is used as part of the Web address pointing to the DataPower SOA appliance. **Restriction:** You cannot specify a path other than `/`. Changing its value has no effect.
–poll *polling interval*	Optional	10 seconds	Defines the DataPower SOA appliance polling interval (in seconds). The data collector waits this amount of time between each poll of the DataPower SOA appliance. This must be an integer value, specified in seconds, between 1 and 300 (1 second to 5 minutes).

Table 58. DataPower key and value pairs for the KD4configDC command (continued)

Parameter	Optional / Required	Default value	Description
-maxrecords *maximum number of records*	Optional	15000	Defines the maximum number of records that the DataPower data collector can process from the DataPower SOA appliance per polling interval. This must be an integer value, between 1 and 30000.
-subexpire *length of time the subscription is valid*	Optional	15	Defines the length of time, in minutes, that the subscription of the DataPower data collector to the DataPower appliance remains valid. At the end of the subscription period, the DataPower data collector renews its subscription to the DataPower appliance. This must be an integer value, specified in minutes, between 3 and 30.
–domainlist *domainA, domainB, ...domainZ*	Optional	No `domainlist` property is generated	Defines the DataPower SOA appliance domain list. This is a comma-separated list of domains to be monitored on the associated DataPower SOA appliance. Any domains in this list that are not authorized to the user defined by the `-user` parameter are not monitored. Each domain can be any string, with no blank characters. If you specify more than one domain name, separated by commas, the entire domain list must be enclosed in double quotation marks (for example, –domainlist "domain1,domain2,domain3". See "Considerations for enabling data collection for DataPower monitoring" on page 468 for more information about using this domain list.
–displaygroup *display group*	Optional	No `displaygroup` property is generated	Defines the DataPower SOA appliance display name. The name can be any string, with no blank characters, up to 64 characters long. See "Creating node names in Tivoli Enterprise Portal" regarding possible truncation of this value in the node name. See "Considerations for enabling data collection for DataPower monitoring" on page 468 for more information about the use of this property.

Important: When you deploy the DataPower data collector, you must start the data collector once you have enabled it to begin collecting data. For more information about starting the data collector, see "Starting and stopping the data collector" on page 474.

Creating node names in Tivoli Enterprise Portal

The DataPower data collector host name is combined with the value of the `–displaygroup` parameter, separated by a hyphen, to form the node name that is seen in the Tivoli Enterprise Portal Navigator view.

For example, the **`KD4configDC`** command is run with the `–displaygroup` parameter specified with a value of `dispName`:

```
KD4configDC -enable -env 8 –host appHost –user user1 –displaygroup dispName
```

In this example, appHost is the host name of the DataPower SOA appliance. The DataPower data collector acts as a proxy on a different computer, and, in this example, proxy host name is dpdcHost. With the –displaygroup parameter specified in the **KD4configDC** command, the node name that is displayed in the Tivoli Enterprise Portal Navigator view is D4:dpdcHost-dispName.

If the –displaygroup parameter is not specified in the **KD4configDC** command, then the value of the –host parameter is used instead of –displaygroup to define the node name.

In the following example, the **KD4configDC** command is run without specifying the –displaygroup parameter:

```
KD4configDC -enable -env 8 –host appHost –user user1
```

The value of the –host parameter (appHost) is combined with the DataPower data collector host name dpdcHost to form the node name that is displayed in the Tivoli Enterprise Portal Navigator view. In this case the node name that is displayed in the Tivoli Enterprise Portal Navigator view is D4:dpdcHost-appHost.

Restriction: If the length of the node name exceeds 20 characters (including the hyphen), the node name is truncated from the end, meaning that the –displaygroup or –host parameter portion is truncated. You should be aware of this limitation of the Tivoli Enterprise Portal and choose values for the –displaygroup and –host parameters of appropriate length, to avoid truncation and possible confusion between similar names.

Examples of configuring for data collection

This section provides several examples of the kinds of monitoring that you can configure by running the **KD4configDC** command using various combinations of parameters.

The simplest form of the command: When you run the **KD4configDC** command to enable monitoring of a DataPower SOA appliance, this is the simplest format of the command:

```
KD4configDC -enable -env 8 –host host –user user
```

For example, with a host name of dpbox1 and a user name of admin, this is the following command:

```
KD4configDC –enable –env 8 –host dpbox1 –user admin
```

The DataPower configuration file is searched for an existing section that matches the specified host and user, and that has no domain list and no display group properties defined.

- If a matching section is found, you are prompted for a password, and the matching section is updated only by encoding the password and storing it in the configuration file for that section.
- If a matching section is not found in the configuration file, you are prompted for a password. A new section of the configuration file is created, with the specified values for the –host, –user and –pswd parameters that are stored in the configuration file for that section.

  No values for –domainlist or –displaygroup parameters are defined, and other optional properties for the section are set to their default values.

Because no value for the –displaygroup parameter is specified, the host name dpbox1 is used as part of the node name that is displayed in the Tivoli Enterprise Portal (for example, D4:dpdcHost-dpbox1).

Specifying domain list or display group parameters: If the –domainlist or –displaygroup parameters are specified in the **KD4configDC** command, they become part of the matching criteria that determines whether the section exists or must be created as new. If a new section must be created, the values that are provided for the –domainlist and –displaygroup parameters are stored in the new section of the configuration file.

For example, if you have two domains, domainA and domainB that you are monitoring on a DataPower SOA appliance defined by a host named host1 and authorized to user userABC, run the **KD4configDC** command:

```
KD4configDC –enable –env 8 –host host1 –user userABC –domainlist "domainA,domainB"
```

The list of domains is surrounded by quotation marks, and there are no blank characters in the domain list.

As another example, suppose you want to create a node name to be displayed in the Tivoli Enterprise Portal Navigator view that contains the display group name of all_domains. This node name would be in the form of D4:dpdcHost-all_domains. Specify these parameters to run the **KD4configDC** command, with authorized user userABC:

```
KD4configDC –enable –env 8 –host host1 –user userABC –displaygroup all_domains
```

Changing existing values for the domain list or display group: To update an existing section of the configuration file by changing the value of either the –domainlist or –displaygroup parameter, you must first disable that section of the configuration file by running the **KD4configDC** command using the –disable parameter (see “Disabling data collection” on page 473), specifying the current values for the –domainlist or –displaygroup parameters.

After the section is disabled, run the KD4configDC command again, using the –enable parameter and specifying the desired values for the –domainlist and –displaygroup parameters.

Specifying the password parameter: The values specified by the –user and –pswd parameters are used to perform an HTTP basic authentication over the HTTPS session. The user and password combination must be a valid user ID and password defined using the administration interface of the DataPower SOA appliance. See the DataPower documentation for more information about creating authorized user names and passwords.

If the –pswd parameter is specified in the **KD4configDC** command, its value is immediately encoded and saved in the configuration file, and you are not prompted for the password. Any password that had previously been specified for an existing section (that matches the search according to the other parameters) is replaced by the new password value.

For example, if an existing section for host name H100 specified an authorized user of u2233, there would already be an encoded value of the valid password stored in the configuration file. To change the password value to x1y2z3, run the **KD4configDC** command:

```
KD4configDC –enable –env 8 –host H100 –user u2233 –pswd x1y2z3
```

Specifying optional parameters: If any of the remaining optional parameters, (–port or –poll) are specified as part of running the **KD4configDC** command, their values are stored in the configuration file in either the existing or newly created section. These values are not used as part of the matching criteria for locating existing sections of the configuration file.

The data collector uses the values in the –host and –port parameters to construct the URL in the form of https://*host*:*port*/. The URL is used as the target of the messages that are sent to the DataPower SOA appliance. Please confirm this update to correct.

Considerations for enabling data collection for DataPower monitoring

You can use variations of the parameters specified in the **KD4configDC** command to define properties that configure the monitoring of one or more DataPower SOA appliances. The following sections illustrate several possible configurations.

Multiple connections to the same DataPower SOA appliance: The DataPower configuration file supports multiple connections to the same DataPower SOA appliance by defining multiple sections of the configuration file with the same host and port properties. There are several reasons why you might want to do this, but the most obvious reason is to allow the data collector to use more than one set of authentication credentials.

For example, a DataPower SOA appliance might have three domains (dom1, dom2 and dom3) and two users (userA, with access only to dom1 and dom2, and userB with access only to dom3).

In this situation, neither userA nor userB can be used to access all of the domains on the appliance. To monitor all of the domains on the appliance, you must define two sections in the DataPower configuration file, one that specifies userA in one section and userB in the other section.

To define the two sections in the configuration file, run KD4configDC command twice, once for each user:

```
KD4configDC –enable –env 8 –host dpHost1 –user userA –domainlist "dom1,dom2"
KD4configDC –enable –env 8 –host dpHost1 –user userB –domainlist dom3
```

Restricting the list of domains being monitored: You can use the –domainlist parameter to restrict the list of domains being monitored for a user. For example, if userA has access to dom1 and dom2, but you are interested in monitoring only dom1, the –domainlist parameter can specify only dom1 to instruct the data collector not to monitor domain dom2:

```
KD4configDC –enable –env 8 –host dpHost1 –user userA –domainlist dom1
```

For each section in the DataPower configuration file, the domains that are monitored depend on the domains to which the user in that section has authorization, and the list of domains specified in the –domainlist parameter for that section. If this property is not specified, then all domains that are authorized to the user for that section are monitored.

Separating and aggregating data with the –displaygroup parameter: The –displaygroup parameter gives you substantial control over how the information from DataPower SOA appliances is separated or aggregated in the Tivoli Enterprise Portal views. Following are some examples of the ways that the –displaygroup parameter can be used to separate or aggregate data.

Separating data by host name or display group: Suppose that you have two DataPower SOA appliances (with different users and domains defined on each) and you want to view the information from these two appliances separately under two different nodes in the Tivoli Enterprise Portal Navigator view.

Because there are two DataPower SOA appliances, there must be at least two sections in the DataPower configuration file, one for each appliance hostname or IP address. Separation of the information from these two appliances can be done without using the –displaygroup parameter if the two sections of the configuration file have different values for the –host parameter. For example:

```
KD4configDC –enable –env 8 –host dpHost1 –user userA
KD4configDC –enable –env 8 –host dpHost2 –user userB
```

The node name that is displayed in the Tivoli Enterprise Portal is based on the value of the –host parameter if the –displaygroup parameter is not specified. As long as the two sections of the configuration file have different values for the –host parameter, ITCAM for SOA separates the data between the two appliances and displays it under two different nodes (for example, D4:dpdcHost-dpHost1 and D4:dpdcHost-dpHost2) in the Tivoli Enterprise Portal Navigator view.

Alternatively, you could use the –displaygroup parameter to specify a more meaningful string than the value of the –host parameter. As long as the values for –displaygroup for the two sections are different, the data is separated under different Tivoli Enterprise Portal Navigator nodes. For example:

```
KD4configDC –enable –env 8 –host dpHost1 –user userA –displaygroup host1Domains
KD4configDC –enable –env 8 –host dpHost2 –user userB –displaygroup host2Domains
```

Because the –displaygroup parameter is specified, the node name is created from those values and should be displayed in the Tivoli Enterprise Portal Navigator view as D4:dpdcHost-host1Domains and D4:dpdcHost-host2Domains. However, note also that in this case, the length of the node name exceeds 20 characters, so each node name is truncated, as D4:dpdcHost-host1Dom and D4:dpdcHost-host2Dom.

Separating data between domains by domain list: Suppose that you have a DataPower SOA appliance with a single user, userA, and two domains, dom1 and dom2.

You can configure the data collector to separate the information from these two domains under two different nodes in the Tivoli Enterprise Portal Navigator view by creating two sections in the DataPower configuration file. The first section specifies a –domainlist parameter of dom1 and a –displaygroup parameter of, for example, Dom1, and the second section specifies a –domainlist parameter of dom2 and a –displaygroup parameter of, for example, Dom2.

Example:

```
KD4configDC –enable –env 8 –host dpHost1 –user userA –domainlist dom1
   –displaygroup Dom1
KD4configDC –enable –env 8 –host dpHost1 –user userA –domainlist dom2
   –displaygroup Dom2
```

The different values for the –displaygroup parameter cause ITCAM for SOA to create two display groups that map to two different Tivoli Enterprise Portal Navigator view nodes: D4:dpdcHost-Dom1 and D4:dpdcHost-Dom2, and the –domainlist parameters restrict the data collected in each of those display groups to just the intended domain, even though userA has access to both domains.

Aggregating data across multiple domains: Suppose that you have a DataPower SOA appliance with a single user, `userA`, and two domains, `dom1` and `dom2`. If the `–displaygroup` parameter is not specified in the section of the configuration file, the node name is created from the `–host` parameter, and the information for both `dom1` and `dom2` is aggregated under a single node (`D4:dpdcHost-dpHost`) in the Tivoli Enterprise Portal Navigator view.

Aggregating data across multiple domains under multiple nodes: To aggregate the data from domains `domA1` and `domB1` under one node name and the data from `domA2` and `domB2` under a different node name, configure four sections in the DataPower configuration file:

- user *userA*, domainlist *domA1*, displaygroup *Group1*
- user *userB*, domainlist *domB1*, displaygroup *Group1*
- user *userA*, domainlist *domA2*, displaygroup *Group2*
- user *userB*, domainlist *domB2*, displaygroup *Group2*

Example:

```
KD4configDC –enable –env 8 –host dpHost –user userA –domainlist "domA1"
   –displaygroup Group1
KD4configDC –enable –env 8 –host dpHost –user userB –domainlist "domB1"
   –displaygroup Group1
KD4configDC –enable –env 8 –host dpHost –user userA –domainlist "domA2"
   –displaygroup Group2
KD4configDC –enable -env 8 –host dpHost –user userA –domainlist "domB2"
   –displaygroup Group2
```

This causes ITCAM for SOA to aggregate the information from `domA1` and `domB1` under the Tivoli Enterprise Portal Navigator node `D4:dpdcHost-Group1` and to aggregate the information from `domA2` and `domB2` under the Tivoli Enterprise Portal Navigator node `D4:dpdcHost-Group2`.

Aggregating data across all domains on a single host with multiple users: Suppose that you have a DataPower SOA appliance with two users (`userA` and `userB`) that each have access to different sets of domains (`userA` has access to domains named `domA1` and `domA2`. The other user, `userB`, has access to domains named `domB1` and `domB2`, respectively). To monitor all of these domains, the DataPower configuration file must have at least two sections, one with a `–user` parameter value of `userA` and one with a `–user` parameter value of `userB`, but each specifying the same value for the host name in the `–host` parameter.

Example:

```
KD4configDC –enable –env 8 –host dpHost –user userA
KD4configDC –enable –env 8 –host dpHost –user userB
```

If the `–displaygroup` parameter is not specified, the information from all four domains would be aggregated under the same Tivoli Enterprise Portal Navigator node, for example, `D4:dpdcHost-dpHost`.

Aggregating data for a cluster of appliances: You might have a collection of DataPower SOA appliances that are identically configured because they are used in a load-balancing or fail over situation. Because each appliance has its own host name or IP address, there must be at least one section in the configuration file for each appliance to inform the data collector how to communicate with each appliance.

If the –displaygroup parameter is not used, then the information for each of these appliances is separated into different nodes in the Tivoli Enterprise Portal Navigator view (for example, D4:dpdcHost-dpHost1), because the –host parameter is used by default.

To see how this *cluster* of appliances is performing as a whole, without regard to the performance of individual appliances, specify the same –displaygroup parameter (for example, Clust1) for every appliance. This causes the data collector to aggregate the data from all of these devices into a single display group, which is then displayed under a single Tivoli Enterprise Portal Navigator node (for example, D4:dpdcHost-Clust1).

Example:

```
KD4configDC –enable –env 8 –host dpHost1 –user userA –displaygroup Clust1
KD4configDC –enable –env 8 –host dpHost2 –user userA –displaygroup Clust1
```

When you specify the –displaygroup parameter for appliances in a cluster, the Application Server Node Name attribute in the Service Inventory_610, the Service Inventory Requester Identity_610, and the Fault Log_610 tables display the name of one of the appliances in the cluster. If you set the DataPower.multihost.group property in the DataPower configuration file to true, the Application Server Node Name attribute is set to empty.

To dimension data for a cluster, you can either dimension the data by display group or by the DataPower appliance host name.

To dimension the data by display group, complete the following steps:

- Set the DataPower.multihost.group property to true.
- Add multiple domains to a single domain list.
- Specify a display group name for the domain list.

For example:

```
DataPower.domainlist.1=example1,example2
DataPower.displaygroup.1=GetCustomer
DataPower.multihost.group.1=true
```

Data from the domains is aggregated based on the display group. The Application Server Node Name in the Service Inventory and Fault Log tables is empty.

To dimension the data by the DataPower appliance host name, complete the following steps:

- Set the DataPower.multihost.group property to false.
- Add each domain to a separate domain list.
- Specify the same display group name for each domain list.

For example:

```
DataPower.domainlist.1=example1
DataPower.displaygroup.1=example
DataPower.dimension.domain.1=true
DataPower.alias.1=alias_102_125
DataPower.multihost.group.1=false

DataPower.domainlist.2=example2
DataPower.displaygroup.2=example
DataPower.dimension.domain.2=true
DataPower.alias.2=alias_102_126
DataPower.multihost.group.2=false
```

Data from the domains is aggregated based on each separate domain. The Application Server Node Name is set to the name of each DataPower appliance.

The `DataPower.multihost.group` property is introduced in ITCAM for SOA version 7.2 Fix Pack 1. For more information, see "The DataPower configuration file" on page 459.

Additional considerations: Take the following into account when considering whether to separate or aggregate data:

Combining configurations

You can mix and match any of the various configurations described in this section, which gives you a great deal of flexibility in defining how to aggregate or separate data in the Tivoli Enterprise Portal views. This flexibility might result in some DataPower domains being specified in more than one section. This is not considered an error.

Duplicated domains

You might want one section defined to allow data for a domain to be displayed on its own under one Tivoli Enterprise Portal Navigator node, and another section (or sections) defined to show the data for that domain aggregated with other domains, on the same or on a different machine. This is possible, but be aware that this results in the data for duplicated domains being retrieved multiple times by the data collector (once for each section in which it is configured). In this situation performance might be affected.

Aggregation defaults

By default, if no `–domainlist` parameter and no `–displaygroup` parameter are used at all in the DataPower configuration file, the DataPower data collector aggregates data for all of the monitored domains on a single DataPower SOA appliance (even if the domains are accessed using different credentials), and keeps the data from each DataPower SOA appliance separated.

Adding appliances to, or removing appliances from display groups

As you define your display groups, you should decide if the display group will always monitor only one appliance or multiple appliances, and once that display group is put into production, do not modify it by adding a second appliance, or by removing appliances to leave only one appliance monitored in the display group.

If your goal in this display group is to monitor a single domain on a single appliance, then after it is put into production, do not add a second appliance to that display group. If your goal is to monitor one domain across a set of appliances, then add at least the second appliance while you are still in development and test mode. After you put this display group into production, ensure that there are always at least two appliances monitored. You can increase from a cluster of two appliances to three or more as needed.

However, if you remove appliances from the display group so that there is only one remaining appliance, the node name attribute changes, and a new subnode identifier is displayed in the Tivoli Enterprise Portal Navigator Physical view. If you modify a display group that contains a single appliance by adding a second appliance, its subnode identifier will also change, and a new subnode with the same name is displayed on the Tivoli Enterprise Portal Navigator Physical view. You must then delete the offline subnode to remove the duplicate names in the view. Any historical data that you collected with the original subnode name is no longer associated with the new subnode name.

Disabling data collection

This section describes the procedures for disabling data collection in the DataPower environment.

To unconfigure the Data Power data collector, you must stop the data collector before disabling it. For more information about stopping the data collector, see "Starting and stopping the data collector" on page 474.

Important: You do not have to stop the data collector first if you are making configuration changes.

Upgrading the data collector

If you are upgrading the data collector for the DataPower environment, *do not* use the `–disable` option of the `KD4configDC` script or the Data Collector Configuration utility described in this section. Instead, you should complete the following steps:

1. Stop the DataPower data collector using the **`stopDC`** command (see "Starting and stopping the data collector" on page 474 for more information.
2. Deregister the service or daemon, if applicable. See "Running the DataPower data collector as a Windows service or UNIX daemon" on page 475 for the procedures to stop a registered DataPower data collector and to deregister the service to remove it from the list of Windows services, if applicable.

See "Upgrading to ITCAM for SOA version 7.2" on page 23 for more information about upgrading your monitoring environment from a previous version.

Disabling data collection using the Data Collector Configuration utility

To disable data collection with the Data Collector Configuration utility, complete the following steps:

1. Run the Data Collector Configuration utility (see "Running the Data Collector Configuration utility" on page 378):
   a. Select the DataPower SOA Appliance runtime environment.
   b. Select the **Configure DataPower Instance** option.
   c. Select the option to disable data collection.

      For the remaining input parameters, refer to Table 58 on page 464 for a description of the information that is required, and see the additional information and examples of running the **`KD4configDC`** command to learn more about how to specify these parameters for your environment.
   d. Specify the DataPower Host Name.
   e. Specify the DataPower user ID.
   f. Specify the DataPower password.
   g. The default DataPower port number (5500) and the default polling interval (10 seconds) is provided. Accept these defaults or type over them to specify different values.
   h. Specify the DataPower Domain List.

i. Optionally specify the DataPower Display Group.
j. Wait for the configuration utility to complete the operation.
k. Exit the utility.

Disabling data collection using the KD4configDC command

When you run the **KD4configDC** command to disable monitoring of a DataPower SOA appliance, use the simplest syntax for running the **KD4configDC** command:

```
KD4configDC –disable –env 8 –host host –user user
```

The DataPower configuration file is searched for an existing section that matches the specified host and user and that has no `–domainlist` parameter and no `–displaygroup` parameters defined. If a matching section is found, the section is removed from the file. If no matching section is found, an error message is issued and the file remains unchanged.

If the `–domainlist` or `–displaygroup` parameters are specified in the **KD4configDC** command, they become part of the matching criteria that determines whether the section exists and whether it is removed if found.

Restriction: If the `-path` parameter is specified, its value is ignored. Instead, the default value of / is used.

All other parameters (`–port`, `–path`, `–poll`, `–maxrecords`, `–subexpire`, or `–password`) are not required and are ignored, if specified on the command line.

Starting and stopping the data collector

Starting the data collector

This section provides the procedures that you can use to start and stop the data collector.

To start the DataPower data collector, open a command-line window, navigate to the *ITM_home*`\TMAITM6\KD4\bin` directory on Windows systems or the *ITM_home*/*platform*`/d4/KD4/bin` directory on Linux and UNIX systems, and run the `startDC` script. Examples:

```
startDC.bat
./startDC.sh
```

Optionally, you can specify the `–background` option to start the data collector proxy as a disconnected task. Examples:

```
startDC.bat -background
./startDC.sh -background
```

Once started, the data collector monitors the console for commands entered by the user.

If you start the data collector by running the `startDC` script in the foreground, you can stop the data collector only by running the **stop**, **quit**, or **exit** command from the command-line window. Any of these commands initiate an orderly shutdown of the DataPower data collector. The data collector waits for all communication sessions to end before the process terminates.

When in background mode or when you inadvertently exit the command-line window in foreground mode, to stop the data collector, navigate to the

ITM_home\TMAITM6\KD4\bin directory on Windows systems or the *ITM_home*/*platform*/d4/KD4/bin directory on Linux and UNIX systems, and run the stopDC script. Examples:

```
stopDC.bat
./stopDC.sh
```

While the data collector is running, you can use the **KD4configDC** command to update the DataPower data collector configuration file and change which DataPower SOA appliances and domains are being monitored. You do not need to stop and restart the data collector to activate these changes. The running data collector detects the changed configuration file within 40 seconds and adjust its monitoring to reflect the updated configuration.

Running the DataPower data collector as a Windows service or UNIX daemon

ITCAM for SOA provides the capability to register and start the DataPower data collector as a service on supported Windows systems, or as a daemon on supported UNIX systems. Running the DataPower data collector in this way improves availability, because the data collector can be automatically restarted in the event of a system restart.

After installing ITCAM for SOA, the DataPower data collector is not automatically registered as a service or daemon, so you can still start the data collector using the startDC script (see "Starting and stopping the data collector" on page 474).

Registering the DataPower data collector as a Windows service or UNIX daemon

To register the DataPower data collector as a Windows service or UNIX daemon, complete the following steps:

1. If the data collector is already started, stop the data collector (see "Starting and stopping the data collector" on page 474).
2. Register the DataPower data collector using either the Data Collector Configuration utility or the **KD4configDC** command.
   - Using the Data Collector Configuration utility:
     a. Start the Data Collector Configuration utility (ConfigDC) from the *ITM_home*\TMAITM6\KD4\bin directory on Windows systems or the *ITM_home*/*platform*/d4/KD4/bin directory on Linux and UNIX systems.
     b. Select the DataPower SOA Appliance runtime environment.
     c. Select the option **Register or unregister DataPower as a service or daemon**.
     d. Select the option **Register DataPower as service or daemon**
     e. The utility reminds you to stop the DataPower data collector before registering it. Click **Next**.
     f. Wait for the operation to complete.
     g. Exit the Data Collector Configuration utility.

     For more information about running the Data Collector Configuration utility, see "Running the Data Collector Configuration utility" on page 378.
   - Using the **KD4configDC** command on Windows systems, run this command:

     ```
     KD4configDC.bat –registerService –env 8
     ```

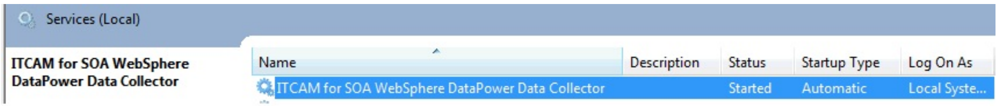
     On AIX, Linux, Solaris, or HP-UX systems, run this command:

```
./KD4configDC.sh -registerService -env 8
```

For more information about running the **KD4configDC** command, see "Running the KD4configDC script" on page 392.

On Windows systems, to verify that the DataPower data collector is registered as a service, complete the following steps:

1. From a command prompt, type **services.msc** to start the `Windows Services Manager`.
2. Locate the **ITCAM for SOA WebSphere DataPower Data Collector** service:



ITCAM for SOA WebSphere DataPower Data Collector

Name	Description	Status	Startup Type	Log On As
ITCAM for SOA WebSphere DataPower Data Collector		Started	Automatic	Local Syste...

Figure 72. Services Utility

3. Verify that the status of the **ITCAM for SOA WebSphere DataPower Data Collector** is set to `Started`.

Starting the registered DataPower data collector

After the DataPower data collector is registered as a service or daemon, it is set to start automatically when the system is rebooted. The data collector is not started immediately, however, in case the data collector is already running in console mode.

To start the DataPower data collector manually for Windows systems, use the Windows Service Manager, or run either of these commands from the *ITM_home*`\TMAITM6\KD4\bin` directory:

```
net start kd4dpdc
startDC.bat [-background]
```

To start the DataPower data collector manually on a Windows system using the Windows Service Manager, complete the following steps:

1. From a command prompt, type **services.msc** to start the `Windows Services Manager`.
2. Locate the **ITCAM for SOA WebSphere DataPower Data Collector** service.
3. Right-click the **ITCAM for SOA WebSphere DataPower Data Collector** service and click **Start**.

To start the DataPower data collector manually for Linux, AIX, Solaris, or HP-UX operating systems, you can run this command from the *ITM_home*`/platform/d4/KD4/bin` directory:

```
./startDC.sh [-background]
```

You can still start the DataPower data collector using the existing `startDC` script. On Windows systems, if the data collector is registered as a Windows service, however, the service starts instead of a console session.

Stopping the registered DataPower data collector

To stop the DataPower data collector manually on Windows systems, use the Windows Service Manager, or run either of these commands from the *ITM_home*`\TMAITM6\KD4\bin` directory:

```
net stop kd4dpdc
stopDC.bat [–background]
```

To stop the DataPower data collector manually on a Windows system using the Windows Service Manager, complete the following steps:

1. From a command prompt, type **services.msc** to start the `Windows Services Manager`.
2. Locate the **ITCAM for SOA WebSphere DataPower Data Collector** service.
3. Right-click the **ITCAM for SOA WebSphere DataPower Data Collector** service and click **Stop**.

To stop the DataPower data collector manually for Linux, AIX, Solaris, or HP-UX systems, run the following command from the *ITM_home*/platform/d4/KD4/bin directory:

```
./stopDC.sh [–background]
```

Removing the DataPower data collector from the list of Windows services

To remove the DataPower data collector from the list of Windows services, complete the following steps:

1. If the data collector is already running, stop it (see "Stopping the registered DataPower data collector" on page 476).
2. Remove the DataPower data collector from the list of Windows services using either the Data Collector Configuration utility or the **KD4configDC** command.
   - Using the Data Collector Configuration utility (see "Running the Data Collector Configuration utility" on page 378):
     a. Start the Data Collector Configuration utility (ConfigDC) from the *ITM_home*\TMAITM6\KD4\bin directory on Windows systems or the *ITM_home*/platform/d4/KD4/bin directory on Linux and UNIX systems.
     b. Select the DataPower SOA Appliance runtime environment.
     c. Select the option **Register or unregister DataPower as a service or daemon**.
     d. Select the option **Unregister DataPower**.
     e. The utility reminds you to stop the DataPower data collector before you unregister it as a service. Click **Next** to continue.
     f. Wait for the operation to complete.
     g. Exit the Data Collector Configuration utility.
   - Using the **KD4configDC** command (see "Running the KD4configDC script" on page 392), run the following command:
     ```
     KD4configDC.bat –deregisterService –env 8
     ```

On Windows systems, to verify that the DataPower data collector is removed from the list of registered service, complete the following steps:

1. From a command prompt, enter **services.msc** to start the `Windows Services Manager`.
2. Verify that the **ITCAM for SOA WebSphere DataPower Data Collector** service is no longer listed in the window.

Deregister before uninstalling the product

When you uninstall ITCAM for SOA, the process does not include removing the DataPower data collector from the list of Windows services. Because this process uses the Data Collector Configuration utility and the **KD4configDC** script, you should always deregister the DataPower data collector Windows service before you uninstall the product.

Error handling

Errors that occur while registering, starting, stopping, or deregistering the service are written to the Windows event log, and also to the Tivoli Monitoring reliability, availability, and serviceability (RAS) logs in the *ITM_Home*\logs directory.

The logfile name follows the Tivoli Monitoring logfile naming convention for ITCAM for SOA, *host_name*_d4_*log_id*.log (for example, omut3_d4_463742c2-01.log). Consult both the Windows event log and the Tivoli Monitoring RAS logs in case of service errors.

For more information about RAS logs, see the logs and data collection for troubleshooting section of the IBM Tivoli Monitoring: Troubleshooting Guide.

Modifying the minimum and maximum JVM heap size

Table 59 presents the recommended JVM heap size setting per transaction rate for the DataPower data collector.

Table 59. Recommended JVM heap size settings per transaction rate

Transaction rate	Recommended heap size
1- 500 transactions per second	256 Mb
501-1000 transactions per second	768 Mb
1001-1500 transactions per second	1280 Mb
1501-2000 transactions per second	1792 Mb

To modify the minimum and maximum JVM heap size of the DataPower data collector, complete the following steps:

1. Stop the DataPower data collector:
   a. On Windows systems, go to the *ITM_home*\TMAITM6\KD4\bin directory and run stopDC.bat.
   b. On Linux and UNIX systems, go to the *ITM_home*/platform/d4/KD4/bin directory and run ./stopDC.sh.
2. Edit the startDC script to modify the JVM heap size.

   On a Windows system, complete the following steps:
   a. Edit the startDC.bat script in a text editor.
   b. Locate the line that starts with set JAVA_OPTS=-Djava.protocol.handler.pkgs=com.ibm.net.ssl.www.protocol. For example:
   ```
   set JAVA_OPTS=-Djava.protocol.handler.pkgs=com.ibm.net.ssl.www.protocol
    -Xms64m -Xmx256m -Xrs
   ```
   c. Modify the value of -Xms<*size*>m parameter to modify the minimum JVM heap size. Modify the value of -Xmx<*size*>m parameter to modify the maximum JVM heap size.
   d. Save the file.

On a Linux or UNIX system, complete the following steps:

a. Edit the ./startDC.sh script in a text editor.

b. Locate the line that starts with JAVA_OPTS="-Djava.protocol.handler.pkgs=com.ibm.net.ssl.www.protocol. For example:

```
JAVA_OPTS="-Djava.protocol.handler.pkgs=com.ibm.net.ssl.www.protocol
 -Xms64m -Xmx256m"
```

c. Modify the value of -Xms<*size*>m parameter to modify the minimum JVM heap size. Modify the value of -Xmx<*size*>m parameter to modify the maximum JVM heap size.

d. Save the file.

3. Start the DataPower data collector:

   a. On Windows systems, go to the *ITM_home*\TMAITM6\KD4\bin directory and run startDC.bat.

   b. On Linux and UNIX systems, go to the *ITM_home*/platform/d4/KD4/bin directory and run ./startDC.sh.

For information about resolving directory path variables, see “Resolving directory path variables” on page xvi.

Important: Modifying the JVM heap size affects the performance of the DataPower data collector.

For more information about stopping and starting the DataPower data collector, see “Starting and stopping the data collector” on page 474.

Configuring the requester identity type for fault monitoring

You can configure the type of requester identity that is displayed in the Fault Details view and the Fault_Log_Table_610 table.

Beginning with ITCAM for SOA version 7.2 Fix Pack 1, a new property is added to the ITCAM for SOA KD4.dc.properties file. The kd4.ira.fault.reqid.type property specifies whether user ID or host IP address are displayed in the Requester Identity attribute in the Fault Details view and in the Fault_Log_Table_610 table.

To configure the type of requester identity to display, complete the following steps:

1. Navigate to the KD4.dc.properties file in the *ITCAM4SOA_Home*/KD4/config directory.
2. Edit the KD4.dc.properties file using a text editor.
3. Set the kd4.ira.fault.reqid.type property to a value of 1, 2, or 3, where:

   1 User ID of the requester.

   2 Host IP address of the requester. The default value is 2.

   3 User ID of the requester. If user ID is not available, then use host IP address.
4. Save your changes in the KD4.dc.properties file.

If you enable service monitoring by requester identity, you might want to view the same requester identity value in the Fault Details view and in the Service Inventory Requester Identity table. To see the same value, you must set the fault and service monitoring requester identity types to the same value.

Remember: For service monitoring, you can set the requester identity type to either of the following values:

- User ID
- Host name or IP address

For more information about configuring requester identity for service monitoring, see “Workspaces for monitoring by requester identity” in the *IBM Tivoli Composite Application Manager for SOA User's Guide*.

Configuring the aggregation of metrics in the Service Inventory Requester Identity table

You can configure whether to aggregate metrics for service providers and requesters in the Services Inventory Requester Identity_610 table.

Beginning with ITCAM for SOA version 7.2 Fix Pack 1, a new property is added to the ITCAM for SOA `KD4.dc.properties` file. The `kd4.ira.reqid.requester.enabled` property specifies whether to aggregate metrics for service providers and service requesters in the Services Inventory Requester Identity_610 table.

To configure the type of aggregation to implement, complete the following steps:

1. Navigate to the `KD4.dc.properties` file in the *`ITCAM4SOA_Home`*`/KD4/config` directory.
2. Edit the `KD4.dc.properties` file using a text editor.
3. Set the `kd4.ira.reqid.requester.enabled` property to a value of `0` or `1`, where:

   0 Aggregates metrics for service providers in the Services Inventory Requester Identity_610 table. The default value if the property is not set is `0`.

   1 Aggregates metrics for service providers and service requesters in the Services Inventory Requester Identity_610 table.
4. Save your changes in the `KD4.dc.properties` file.

Communicating between data collector and appliance

Approximately every 10 minutes, the data collector queries the DataPower SOA appliance to see if the domain list has changed. If the domain list has changed, the data collector updates its information as needed and begins monitoring new domains defined on the Data Power appliance.

The data collector polls for data at a frequency that is defined by the `–poll` parameter (the default is 10 seconds).

Communication errors between the data collector and the DataPower SOA appliance that prevent the collection of data are logged to the console (the command-line session where the `startDC` script was executed) and to the operations log. If the data collector is running in background mode, errors are written to the operations log. Additional information concerning the communications between the data collector and DataPower SOA appliance can be obtained by setting the operations logging level for the data collector from `error` to `info` using the `updateLogging` Take Action command from the Tivoli Enterprise Portal.

Optimizing performance

Techniques for optimizing the performance of data collection and data processing are described in the following sections.

Optimizing the performance of data processing

The data collector is configured by default to monitor all services and operations, but with no logging of message content. This configuration optimizes the performance of processing data by not having to handle message content when it is not needed. When you modify any monitor controls to specify a content logging setting other than *none*, all of the full message content for all services and operations is retrieved from the appliance, and the data collector applies the configured monitor control rules (`headers/body/full`) by service and by operation.

See "Configuring the XML Management Interface" on page 446 for information about configuring the `CaptureMode` setting.

Optimizing the performance of data collection

The data collector is configured by default to poll the DataPower SOA appliance every 10 seconds for transaction records. By default, the data collector is configured to process a maximum of 15,000 transaction records during each polling interval. You can increase this value up to a maximum of 30,000 transaction records.

You can modify the polling interval and the number of records processed during the polling interval in line with the transaction volumes on your DataPower appliance. Modifying these properties provides the DataPower data collector with more control over the number of transaction records that it processes and helps to maximize the performance of the data collector.

In the `KD4.dpdcConfig.properties` file, the `DataPower.poll` property specifies the polling interval and the `DataPower.maxrecords` property specifies the maximum number of records to process per polling interval. Both properties are optional.

The combined values of the polling interval and the maximum number of records specifies a transaction rate for data collection. For example, to specify a transaction rate of 1,000 transaction records per second, set the `DataPower.maxrecords` property to 1000 and set the `DataPower.poll` property to 1.

You might observe record loss when you set the maximum number of records to retrieve to too low a value for your environment. On the DataPower appliance, if the number of records in the WSM buffer exceeds the maximum record size limit of the buffer, records might be lost. If you observe high bursts of traffic on your DataPower appliance, you might decide to increase the maximum record size limit of the buffer. For more information about modifying the maximum record size limit of the buffer, see "Configuring the XML Management Interface" on page 446.

Depending on your deployment, you might observe high CPU usage on the system where the data collector is installed during the processing of transaction data from the DataPower appliance when the maximum number of records is set to too high a value or when the polling interval is too frequent, or both.

To prevent high CPU usage and data loss from occurring, tune the polling interval and the maximum number of records for your DataPower deployment.

To modify the DataPower.poll and the DataPower.maxrecords properties, issue the KD4configDC command with the -maxrecords and -poll parameters. For example:

```
KD4configDC -enable -env 8 –host appHost –user user1 -poll 1 -maxrecords 1000
```

Restriction: In an upgrade scenario, to set the maximum number of records for an existing display group, you must add the DataPower.maxrecords property manually to section in the KD4.dpdcConfig.properties file that configures the display group.

For more information about issuing the KD4configDC command, see "Enabling data collection using the KD4configDC command" on page 463.

If you observe that CPU usage is high on the system where the data collector is running, you can also increase the maximum JVM heap size to improve the performance of the data collector. To modify the maximum JVM heap size, see "Modifying the minimum and maximum JVM heap size" on page 478.

Limitations

You can control the monitoring to limit the collection of data to specific services and operations, but you cannot use filter controls to reject messages of specific services or operations. To filter (reject) messages, use the Policy Rules and Actions of the DataPower Web Services Proxy configuration.

If the transforms are not activated, the data collector does not generate a meaningful correlator for messages flowing through the DataPower SOA appliance, so this data does not render properly in the topology, sequence diagram, and pattern views in the IBM Web Services Navigator. For more information, see "Configuring processing rules for DataPower Web Services Proxy gateways" on page 447.

The DataPower data collector creates metric, content, operation and trace log files, but because message filtering is not supported, it does not create any action log files.

Depending on your configuration, the data collector creates multiple metric and content log files to describe the existence of several different display groups. Each display group is represented as a separate node in the Tivoli Enterprise Portal Navigator view. The log files for each display group hold the data for all of the DataPower SOA appliances that are configured for that display group, which might span multiple DataPower domains and include data from multiple DataPower SOA appliances.

Before you attempt to delete an application domain from DataPower that is being monitored by the DataPower data collector, you must either run the **KD4configDC** command to disable monitoring of that application domain, or stop the data collector. Otherwise, when you attempt to delete the domain using the DataPower administration console, you receive an error and the domain cannot be deleted.

Troubleshooting

If you encounter a communication problem, time synchronization problems, or password problem, refer to the information in the following sections to help resolve the problem.

For more information about resolving problems with the DataPower data collector, see the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide*.

Communication failures

If a communications failure occurs, the data collector attempts to initialize itself again and reestablish communication with the target DataPower SOA appliance after the next polling interval (the polling interval is specified by the `–poll` parameter). This process is repeated each polling interval until communication is successfully reestablished, or until the data collector is stopped. Setting the operations logging level to `info` gives you the best indication of status of the communications between the data collector and the appliance.

Synchronizing time between computer systems

For data to display properly in the Tivoli Enterprise Portal, the DataPower SOA appliance, the data collector system, and the Tivoli Enterprise Monitoring Server system must have their clocks synchronized within 5 minutes of each other, in terms of the UTC time they report.

Password problems

User IDs and passwords for DataPower SOA appliances are created and maintained at the appliance. See the documentation that is provided with your DataPower SOA appliance for information about creating and managing user IDs and passwords. When you have reset this information at the DataPower SOA appliance, use the **`KD4configDC`** command to update the DataPower configuration file with the latest user ID and password values for the appropriate section of the file.

Logging and Tracing

The data collector in the DataPower environment uses the same operation and trace log files as other environment types supported by ITCAM for SOA, but rather than creating separate operation and trace files for each display group, it creates a single operation file and a single trace file for all display groups.

The view in the Tivoli Enterprise Portal continues to operate as though you can configure logging and tracing for each display group, but the settings for all DataPower display groups are considered when the settings for the single log or trace writer instance are initialized, as follows:

- If any display group has trace set to *ON*, the DataPower data collector records tracing information for all display groups to the trace log.
- The DataPower data collector uses the lowest severity log setting (*Info*, *Warning*, or *Error*) of all display groups to determine what messages it records in the operations log. For example, if a display group has a log setting of *Info*, then all informational, warning, and error messages for all display groups are written to the operations log.

The DataPower data collector does not update the global configuration settings seen in the Tivoli Enterprise Portal to reflect the actual settings being used for the various display groups. As a result, the Tivoli Enterprise Portal might still show different log and trace settings for each display group, even though the data collector is using common settings for all display groups.

In addition to the operations log, the DataPower data collector issues messages to the console where the `startDC` script was run. All messages issued to the console are also recorded in the operations log. In background mode, information is written to the operations log. On Windows, errors might also be displayed in the Windows Application Event log.

(Optional) Verifying that the configuration of the data collector

After you have verified that the ITCAM for SOA agent has been installed and configured, you might want to verify that your DataPower data collector is configured correctly and monitoring data. To verify the configuration of your data collector, complete these additional tasks.

Verifying that the DataPower data collector is configured and started

Complete the following steps:

1. Verify that the DataPower data collector is started.

   When the data collector is started, an operations log is created. The operations log is in the *ITCAM4SOA_Home*\KD4\logs directory on Windows systems and in the *ITCAM4SOA_Home*/KD4/logs directory on Linux and UNIX systems. If there is no operations log, you must start the DataPower data collector (see "Starting and stopping the data collector" on page 474). If the data collector fails to start, check the operations log for failures. Communication failures or login failures are recorded in the operations log.
2. Verify that the DataPower data collector properties file, `KD4.dpdcConfig.properties`, exists.

   The properties file is created when you enable data collection for one or more DataPower appliances using either the Data Collector Configuration utility or the **KD4configDC** command (see "Enabling data collection" on page 459).

   The properties file is in the *ITCAM4SOA_Home*/KD4/config directory on Linux or UNIX systems and in the *ITCAM4SOA_Home*\KD4\config directory on Windows systems.
3. Verify that the content of the properties file matches the configuration changes that you made using the Data Collector Configuration utility or the **KD4configDC** command. Make sure that the connection to each DataPower appliance is configured correctly in this file:
   - Each section of the file represents a connection to a single DataPower SOA appliance. For each connection, the file stores the host name, port, user ID, and password that is needed to communicate with the device.
   - Each section of the file might specify the domains to monitor on the appliance.
   - Each section of the file might specify a display group that data from the appliance is displayed under in the Tivoli Enterprise Portal.

   For example:

   ```
   # Sample DataPower data collector configuration file
   DataPower.count=1
   #
   DataPower.host.1=dpbox1
   DataPower.port.1=5550
   DataPower.path.1=/
   DataPower.poll.1=60
   DataPower.user.1=admin
   DataPower.encpswd.1=#$%*&
   DataPower.domainlist.1=default,testdom1
   DataPower.displaygroup.1=dpbox1
   DataPower.subExpire.1=15
   ataPower.maxrecords.1=1000
   ```

   The property `DataPower.count` represents the number of DataPower appliances that are configured in the properties file. Verify that its value matches the number of sections in the file.

4. Verify that the user ID and passwords that are specified in the connection properties for each DataPower SOA appliance are correct.

   To ensure that the password has not expired and that the user credentials have been used at least once to the log in to the appliance, log in to the DataPower WebGUI using the user ID and password configured in the properties file.

Verifying that the DataPower appliance is storing transaction data

Complete the following steps:

1. Confirm that the DataPower SOA appliance is configured to store data about business requests in the WSM agent that is associated with each domain:
   a. Confirm that Web Service Management option is selected for the DataPower XML Management Interface object.
   b. If you want to save metric records when the data collector is not started, from the WebGUI, navigate to **Objects** > **Device Management** > **Web Services Management Agent**. Verify that the WSM buffering mode option on the DataPower appliance is set to `Buffer` for each domain.

   For more information about setting the Web Service Management option, see "Configuring the DataPower SOA appliance for monitoring" on page 445.
2. Verify that traffic is flowing through the DataPower device.

   From the WebGUI, navigate to **Status** > **Web Service** > **Web Services Operation Metrics** to verify that metrics are being generated. Traffic must be associated with the domains specified in the domain list in the properties file.
3. Verify that each WSM agent on the DataPower appliance is storing data about the request and response messages.

   To view the status of a WSM agent from the WSM Agent Status page, from the WebGUI, navigate to **Status** > **Web Service** > **WSM Agent Status**. The page displays the status of the WSM agent for each domain, for example:

   ```
   Active Subscribers:0
   Records Seen: 1049
   Records Lost: 0
   Pending Records: 3
   Complete Records: 87
   ```

   Where:

   `Records Seen`
   When a transaction is processed for a domain by the DataPower Web Service Proxy, the `Records Seen` count increments by 1.

   `Records Lost`
   The number of records that are discarded when the buffer is full.

   `Records Pending`
   The number of requests that are waiting on a server response.

   `Complete Records`
   The number of transactions that are ready for collection. This number reduces each time ITCAM for SOA collects data from the DataPower appliance.

   `Active Subscribers`
   The `Active Subscribers` count increases from 0 to 1 when ITCAM for SOA collects data from the WSM. When ITCAM for SOA has collected the data, the number of complete records decreases to 0.

Remember: When you reboot the appliance, the counters are reset.

Verifying that metric log files are generated

Complete the following steps:

1. Verify that metric log files are generated for the DataPower appliance.

   Navigate to the *ITCAM4SOA_HOME*\KD4\logs directory on Windows systems or the *ITCAM4SOA_HOME*/KD4/logs directory on UNIX or Linux systems and verify that a metric file was created for the DataPower data collector in the format: `KD4.8.`*`hostname.domain_name.display_group`*`.metric.log`.
2. Verify that logs are being moved to the *`ITCAM4SOA_HOME`*`\KD4\logs\KD4.DCA.CACHE` directory on Windows systems or the *`ITCAM4SOA_HOME`*`/KD4/logs/KD4.DCA.CACHE` directory on Linux or UNIX systems approximately every 10 seconds after the contents of the file are read by the monitoring agent. If the files are not moved, the monitoring agent might not be running.
3. If you want to collect message content in addition to summary metrics, verify that the **CaptureMode** setting is set to `all-messages` for each domain that you are monitoring. To verify this setting, from the WebGUI, navigate to **Services** > **Miscellaneous** > **Web Services Agent**.

Verifying that web service proxy is configured correctly

Complete the following steps:

1. If you are monitoring traffic through a web service proxy, verify that traffic is being processed by the WS-proxy service on the Data Power SOA appliance.
   a. Log in to the administration console as admin in the default domain.
   b. Navigate to **Status** > **Web Service** > **Web Service Operation Metrics**. This page shows the number of times each operation has been invoked since the service was restarted. If this page does not show increasing counts, then this service is not the service that is being invoked.
2. Verify that performance summary metrics and topology data are displayed for the web service proxy in the Tivoli Enterprise Portal.

   If topology data is not displayed, the processing rules for the web service proxy might not be configured correctly. The correlator that is used to track topology data is not processed automatically by the web service proxy. You must add some transforms, which are included in your DataPower firmware, to the processing rules to handle the correlator.

For more information about configuring processing rules for the web service proxy, see "Configuring processing rules for DataPower Web Services Proxy gateways" on page 447.

Verifying that the multi-protocol gateways are configured correctly

Verify that processing rules have been configured for monitoring traffic through the multi-protocol gateway. No monitoring of the multi-protocol gateways occurs until these processing rules have been added. Unlike the web service proxy, no default transforms are provided with the device. Instead, your application developers must add additional logic to the processing rules based on sample style sheets that are provided to correlate request and response messages and to add the data collected to the WSM for collection by ITCAM for SOA.

If you are monitoring a multi-protocol gateway, inspect the processing rules manually to confirm that the correlator is being calculated on the request and response messages, that the transaction data collected is sent to the WSM agent for ITCAM for SOA to collect, and that the necessary transforms have also been added for processing error message.

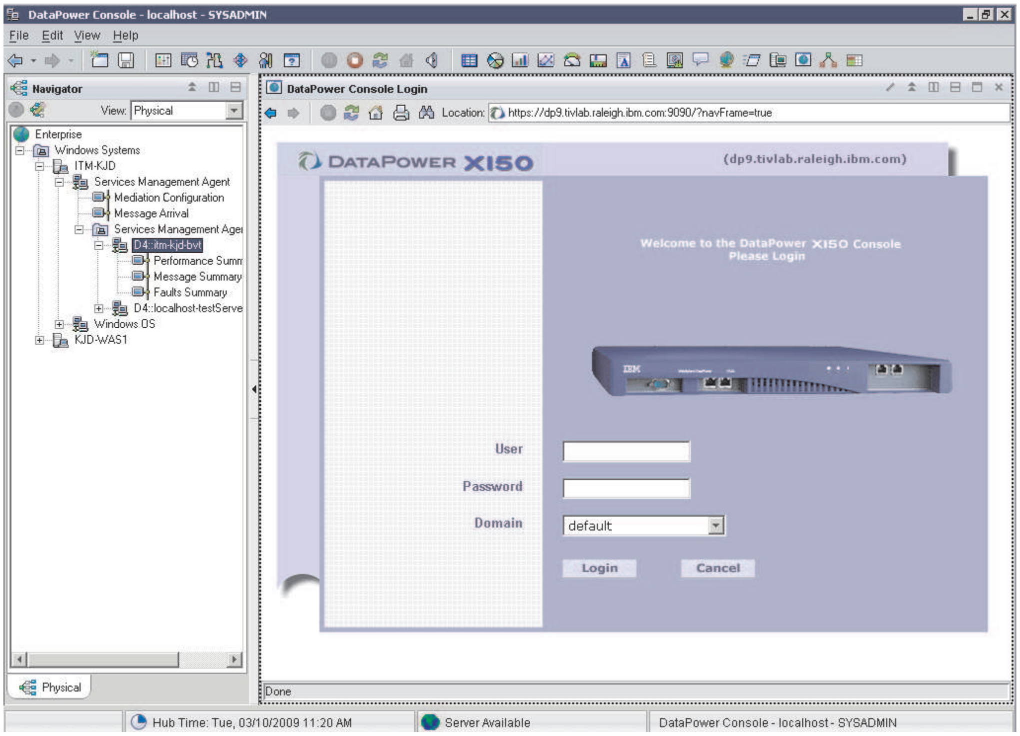
For more information about configuring processing rules for the multi-protocol gateway, see "Configuring processing rules for DataPower Multi-Protocol Gateways" on page 449.

Displaying the DataPower Console interface

You can select a DataPower SOA appliance that is displayed in a row of the Services Inventory attributes table in the Performance Summary workspace of the Tivoli Enterprise Portal, or select an instance of a DataPower mediation operation from one of the Operational Flow displays, and follow the procedure described in this section to display the DataPower Console user interface in a Tivoli Enterprise Portal view. You can then use this interface to configure the DataPower SOA appliance and the policies that the appliance applies to services traffic.

To display the DataPower Console user interface, complete the following steps:

1. From the Tivoli Enterprise Portal, navigate to the Performance Summary workspace and display the Services Inventory attributes table view.
2. Select a row in the table from the DataPower system referenced in the **Node Name** column, and click the link icon to select the DataPower Console option. The DataPower Console is displayed in a Tivoli Enterprise Portal view, similar to the example shown in Figure 73.



DataPower Console - localhost - SYSADMIN

View: Physical

Location: https://dp9.tivlab.raleigh.ibm.com:9090/?navFrame=true

Welcome to the DataPower XI50 Console
Please Login

Domain: default

Hub Time: Tue, 03/10/2009 11:20 AM

Figure 73. The DataPower Console

Considerations when displaying the DataPower Console view

Additional limitations, restrictions, and considerations to keep in mind as you launch the DataPower Console user interface are presented in the following sections:

Start only from a row that represents a DataPower environment

You cannot start a DataPower Console session from a row in the Services Inventory attributes table that represents a non-DataPower application server runtime environment. DataPower SOA appliances are identified by a value of *DataPower* in the Application Server Environment column of the Services Inventory attributes table.

If you select a row that does not represent metrics data from a DataPower application server runtime environment, a browser session is started with the `KD4LN0001E` error message displayed.

If you select a row that does not represent a DataPower appliance, the link to the DataPower Console is not displayed.

Cannot start from a row with aggregated DataPower metrics

Because of how the data collector works and the way that the **Application Server Node Name** field is populated by the DataPower data collector, you cannot display the DataPower Console from a Services Inventory attributes table row that represents metrics aggregated from more than one physical DataPower SOA appliance.

In the case of aggregated metric data from more than one DataPower SOA appliance, the **Node Name** field is blank to prevent possibly displaying the DataPower Console for the wrong DataPower SOA appliance. If you select a row in the table that represents metrics aggregated from more than one physical DataPower SOA appliance, a browser session is started with error message `KD4LN0002E` displayed.

The DataPower Console must be configured for Port 9090

The link to the DataPower Console operates correctly only if the DataPower Console is configured for port `9090` (port 9090 is also the default port number). See the *DataPower WebGUI Guide* and the *DataPower CLI Reference Guide* for information about configuring the port.

Logging in to DataPower

If you have not previously logged in to the DataPower Console user interface in the current browser session, the web browser session opens with the login page. You need to log in with a valid user name and password to continue. If you have previously logged in, the session opens with the main page of the user interface.

See your DataPower documentation for more information about user names and password, and consult your local system administrator for assistance if needed.

Chapter 18. Integrating with ITCAM for Transactions

The Microsoft .NET and DataPower data collectors support native integration with ITCAM for Transactions.

When ITCAM for SOA is integrated with ITCAM for Transactions, Microsoft .NET and DataPower transaction data is sent to the Transaction Collector server, which stores tracking data from multiple data collectors and aggregates this data for display in Transaction Tracking workspaces in the Tivoli Enterprise Portal.

Remember:

- When you integrate the DataPower data collector with ITCAM for Transactions, you must add preloaded transforms to your processing rules if you are monitoring a web services proxy. Also, if you are monitoring a multi-protocol gateway, you must add additional logic to your transforms. For more information about configuring processing rules, see "Configuring DataPower Processing Rules" on page 447.
- The Microsoft .NET data collector refers to the .NET data collectors provided by ITCAM for SOA version 7.2 and later and ITCAM for Microsoft Applications version 6.3 and later.

ITCAM for SOA provides the following three ways to integrate the Microsoft .NET, and DataPower data collectors with ITCAM for Transactions:

- The `KD4configureTT` command-line utility
- The Data Collector Configuration Utility
- By modifying the `KD4.dc.properties` file

Important:

- You can integrate the WebSphere Application server data collector, ITCAM Data Collector for WebSphere, with ITCAM for Transactions. The ITCAM Data Collector for WebSphere configuration utilities provide an option to integrate the data collector with ITCAM for Transactions. For more information, see "Communicating with ITCAM for Transactions" on page 272.
- You can integrate the Data Collector for WebSphere Message Broker with ITCAM for Transactions. To integrate the data collector with ITCAM for Transactions, see "Integrating the data collector with ITCAM for SOA and ITCAM for Transactions" on page 368.
- You must not configure data collection for .NET environments for the ITCAM for SOA from either of the following products simultaneously on the one system:
  - ITCAM for Transactions
  - ITCAM for Microsoft Applications
  - ITCAM for SOA component in ITCAM for Applications

Integrating with the Transactions Collector using the `KD4configureTT` utility

The `KD4configureTT` utility is used to set the address of the Transaction Collector server and to enable or disable the data collector to send transaction tracking API events from ITCAM for SOA to the Transaction Collector server.

The KD4configureTT utility is in the *ITM_home*\TMAITM6\KD4\bin directory on Windows systems and in the *ITM_home/platform_name*/d4/KD4/bin directory on Linux and UNIX systems.

The syntax of the KD4configureTT utility is as follows:

```
KD4ConfigureTT -enable|-disable [-server Transaction_Collector_server_address]
```

Where:

-enable
Enables the data collectors to send transaction tracking API events to the Transaction Collector.

-disable
Disables the data collectors to send transaction tracking API events to the Transaction Collector.

-server
Specifies the address and port number of the Transaction Collector server. The address must be of the format *tcp*:*hostname*:*port* or *tcp*:*IP_address*:*port*.

On Windows systems, launch the utility by running KD4configureTT.bat. On UNIX, launch the utility by running KD4configureTT.sh.

Integrating with the Transactions Collector using the Data Collector Configuration utility

The Data Collector Configuration utility is in the *ITM_home*\TMAITM6\KD4\bin directory on Windows systems and in the *ITM_home/platform_name*/d4/KD4/bin directory on Linux and UNIX systems. The utility can also be used to enable and disable the data collectors to send transaction events to ITCAM for Transactions. Run the Data Collector Configuration utility using the following general format on Windows systems:

```
ConfigDC.bat [–console | –silent [dir_path/]silent_file]
[–debug [dir_path/]debug_file]
```

Use the following format on UNIX or Linux systems:

```
./ConfigDC.sh [–console | –silent [dir_path/]silent_file]
[–debug [dir_path/]debug_file]
```

The KD4.dc.properties file is in *ITM_Home*\TMAITM6\KD4\config directory on Windows systems or the *ITM_Home/platform_name*/d4/KD4/config directory on Linux and UNIX systems.

For more information about displaying ITCAM for SOA data in Transaction Tracking workspaces, see the *IBM Tivoli Composite Application Manager for Transactions Installation and Configuration Guide*.

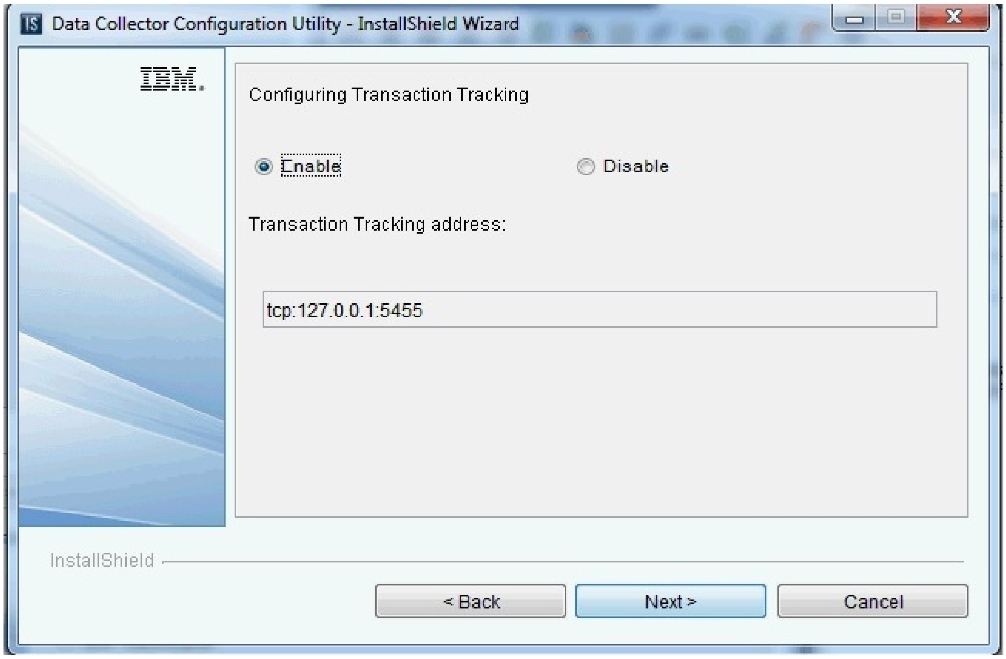
Enabling the interface to ITCAM for Transactions

To enable the sending of transaction tracking API (TTAPI) events to the Transaction Collector, run either the Data Collector Configuration Utility or the KD4configureTT command-line utility, or modify the contents of the KD4.dc.properties file.

Enabling the TTAPI using the Data Collector Configuration utility

Complete these steps:

1. Change to the *`ITM_Home`*`\TMAITM6\KD4\bin` directory on Windows systems or the *`ITM_Home`*`/`*`platform_name`*`/d4/KD4/bin` directory on Linux and UNIX systems.
2. Enter the command`ConfigDC.bat` on Windows systems or `ConfigDC.sh` on Linux or UNIX systems to start the utility.
3. Select the option to Configure Transaction Tracking settings and click **Next**.
4. Select the option to enable transaction tracking. For example:



Configuring Transaction Tracking

● Enable ○ Disable

Transaction Tracking address:

tcp:127.0.0.1:5455

Figure 74. Configuring Transaction Tracking

5. Specify the IP address or host name of the Transaction Collector.
6. Specify the port number of the Transaction Collector server on which to listen for transaction events. The default port number is `5455`.
7. Click **Next** to enable transaction tracking.
8. Exit the utility.

Enabling the TTAPI using the `KD4configureTT` utility

Complete these steps:

1. Change to the *`ITM_Home`*`\TMAITM6\KD4\bin` directory on Windows systems or the *`ITM_Home`*`/`*`platform_name`*`/d4/KD4/bin` directory on Linux and UNIX systems.
2. Enter the command `KD4configureTT.bat -enable [-server` *`Transaction_Collector_server_address`*`]` on Windows systems or `./KD4configureTT.sh -enable [-server` *`Transaction_Collector_server_address`*`]` on Linux or UNIX systems to enable the transaction tracking interface.

   For example:

   ```
   KD4configureTT.bat -enable -server tcp:collector.ibm.com:5455
   ```

   In this example, ITCAM for SOA sends transaction tracking API events to the default port `5455` on host `collector.ibm.com`.

Enabling the TTAPI by modifying the `KD4.dc.properties` file

Complete these steps:

1. Change to the *ITM_Home*\TMAITM6\KD4\config directory on windows or the *ITM_Home*/*platform*/d4/KD4/config directory on Linux and UNIX systems.
2. Open the KD4.dc.properties file in the current directory.
3. To enable the transaction tracking interface, set the following properties:

   ```
   default.tt.enabled=true
   default.tt.serverstring=Transaction_Collector_server_address
   ```

   Set the *Transaction_Collector_server_address* in the format of *tcp*:*hostname_or_IP_address*:*port*. For example:

   ```
   default.tt.enabled=true
   default.tt.serverstring=tcp:127.0.0.1:5455
   ```

Configuring TTAPI for a single web service for the .NET data collector

Complete these steps:

1. Change to the *ITM_Home*\TMAITM6\KD4\config directory on Windows systems or the *ITM_Home*/*platform*/d4/KD4/config directory on Linux and UNIX systems.
2. Open the KD4.dc.properties file in the current directory.
3. To enable the transaction tracking interface for a single web service for the .NET data collector, set the following properties:

   ```
   default.tt.enabled=false
   2.WEBSERVER.tt.enabled=true
   2.WEBSERVICE.tt.serverString= Transaction_Collector_server_address
   ```

   Set the *Transaction_Collector_server_address* in the format of *tcp*:*hostname_or_IP_address*:*port*. For example:

   ```
   default.tt.enabled=false
   2.WEBSERVER.tt.enabled=true
   2.WEBSERVICE.tt.serverString=tcp:127.0.0.1:5455
   ```

Configuring TTAPI for a single DataPower display group

Complete these steps:

1. Change to the *ITM_Home*\TMAITM6\KD4\config directory on Windows systems or the *ITM_Home*/*platform*/d4/KD4/config directory on Linux and UNIX systems.
2. Open the KD4.dc.properties file in the current directory.
3. To enable the transaction tracking interface for a single DataPower display group, set the following properties:

   ```
   default.tt.enabled=false
   8.DisplayGroup.tt.enabled=true
   8.DisplayGroup.tt.serverstring=tcp:127.0.0.1:5455
   ```

Disabling the interface to ITCAM for Transactions

To disable the sending of transaction tracking API (TTAPI) events to the Transaction Collector, run either the Data Collector Configuration Utility or the KD4configureTT command-line utility, or modify the contents of the KD4.dc.properties file.

Disabling the TTAPI using the Data Collector Configuration utility

Complete these steps:

1. Change to the *ITM_Home*\TMAITM6\KD4\bin directory on Windows systems or the *ITM_Home*/*platform*/d4/KD4/bin directory on Linux and UNIX systems.
2. Enter the command ConfigDC.bat on Windows systems or ConfigDC.sh on UNIX or Linux systems to start the utility.
3. Select the option to configure transaction tracking settings.
4. Select the option to disable transaction tracking.
5. Click **Next** to disable transaction tracking.
6. Exit the utility.

Disabling the TTAPI using the KD4configureTT utility

Complete these steps:

1. Change to the *ITM_Home*\TMAITM6\KD4\bin directory on Windows systems or the *ITM_Home*/*platform*/d4/KD4/bin directory on Linux and UNIX systems.
2. Enter the command KD4configureTT.bat -disable [-server *Transaction_Collector_server_address*] on Windows systems or ./KD4configureTT.sh -disable [-server *Transaction_Collector_server_address*] on Linux or UNIX systems to disable the transaction tracking interface.

   ```
   KD4configureTT.bat/sh -disable
   ```

Disabling the TTAPI by modifying the KD4.dc.properties file

Complete these steps:

1. Change to the *ITM_Home*\TMAITM6\KD4\config directory on Windows systems or the *ITM_Home*/*platform*/d4/KD4/config directory on Linux and UNIX systems.
2. Open the KD4.dc.properties file in the current directory.
3. To disable the transaction tracking interface, set the default.tt.enabled property to false. For example:

   ```
   default.tt.enabled=false
   ```

Part 5. Completing your installation

At this point you should have completed all the appropriate steps in Part 1, “Installing the product,” on page 1 to install application support files and the monitoring agent in your Tivoli Monitoring environment.

If you are using the topology support for service registry and business process integration or service-to-service topology workspaces and views, you should have already configured SOA Domain Management Server and Tivoli Common Object Repository topology support.

You should have configured your various runtime environments for data collection on each computer in your environment where services are being monitored, using the information in Part 4, “Configuring ITCAM for SOA-specific data collectors for runtime environments,” on page 373 of this guide.

Use the remaining information in this part of the guide to complete the basic installation steps and verify the configuration.

See also the *IBM Tivoli Composite Application Manager for SOA Troubleshooting Guide* for information about recovering from problems you might encounter while performing the installation.

Chapter 19. Enabling historical data collection

Data collected by the ITCAM for SOA monitoring agent can be stored long term in the Tivoli Data Warehouse. A number of applications access this data for inclusion in their displays:

- IBM Web Services Navigator retrieves the data from the Tivoli Data Warehouse and converts the data into a format that can be displayed in an Eclipse-based viewer.
- Tivoli Common Reporting retrieves the data from the Tivoli Data Warehouse for display in the HTML or PDF reports it generates.
- The Tivoli Enterprise Portal retrieves data from the Tivoli Data Warehouse and incorporates this data in its workspaces.

Data collected by the ITCAM for SOA monitoring agent is stored at intervals in short-term history files. If historical data collection is configured for ITCAM for SOA, the monitoring server sends this data to the warehouse proxy agent at regular intervals. The warehouse proxy inserts the data it receives into the Tivoli Data Warehouse. To enable historical data collection for ITCAM for SOA, you must configure the warehouse proxy agent and enable historical data collection on ITCAM for SOA attribute groups. For information about configuring the warehouse proxy, see the *IBM Tivoli Monitoring: Installation and Setup Guide*. When this configuration is complete, the Tivoli Enterprise Monitoring Server begins processing the locally stored log files of services data on each application server and sends the data to the warehouse database.

Tip: The mechanism for configuring historical data collection changed in IBM Tivoli Monitoring version 6.2.2. You no longer explicitly start and stop historical data collection for an attribute group. You must also explicitly distribute the historical data collection attribute group settings to your monitoring agent.

Remember: If you configured historical data collection in ITCAM for SOA version 7.1.1, after you upgrade to version 7.2, data is not viewable in the Tivoli Enterprise Portal until one of the following conditions occurs:

- The Warehouse Proxy Agent exports its first batch of data for a specific attribute group.
- The Summarization and Pruning agent runs for the first time after the upgrade to ITCAM for SOA version 7.2.

Considerations for historical data collection on ITCAM for SOA

The Web Services Navigator, Tivoli Enterprise Portal, and Tivoli Common Reporting can be configured to retrieve historical data for ITCAM for SOA agents from the Tivoli Data Warehouse for display in views, workspaces, or reports. The location where the historical data is to be displayed by these applications determines the set of attributes that must be enabled:

Table 60. Attribute groups to configure for historical data collection

Display Location	Attribute groups
IBM Web Services Navigator - All Views	• Relationships • Environment_Mapping • Svc_Port_Oper_Mapping • Service_Flow_Metrics
Tivoli Enterprise Portal Service-to-Service topology workspaces	• Rel_Resp_Metrics • Rel_Req_Metrics
• Tivoli Enterprise Portal - Performance Summary workspaces • ITCAM for SOA reports in Tivoli Common Reporting	Services_Inventory_610
• Performance Summary for Requester Identity workspace • ITCAM for SOA reports in Tivoli Common Reporting	Services_Inventory_ReqID_610
• Tivoli Enterprise Portal - Fault Summary workspace • ITCAM for SOA reports in Tivoli Common Reporting	Fault Log_610

You have to enable history collection for attribute groups used by the IBM Web Services Navigator only if the Navigator is used to import data from the data warehouse (the IBM Web Services Navigator can also import data from metric log files).

Important: Do not enable history collection for both the `Services_Flow_Metrics` attribute group and `Services_Message_Metric_610` table as this impacts the ITCAM for SOA agent's performance.

When configuring historical data collection, you must also consider the length of time for which you want to save data (*pruning*) and how often you want to aggregate detailed data (*summarization*) in the Tivoli Data Warehouse.

Table 61 shows the general recommendations for pruning and summarization of ITCAM for SOA attribute groups, based on the anticipated volume of data in each attribute group.

Table 61. Recommendations for summarization and pruning of ITCAM for SOA attribute groups

Attribute group name	Summarize	Prune
ServicesInventory_610	Yes	Yes
ServicesInventoryReqID_610	Yes	Yes
EnvironmentMapping	No	No
Rel_Resp_Metrics	No	Yes
Rel_Req_Metrics	No	Yes
Relationships	No	No
Service_Flow_Metrics	No	Yes

Table 61. Recommendations for summarization and pruning of ITCAM for SOA attribute groups (continued)

Attribute group name	**Summarize**	**Prune**
SVC_Port_Oper_Mapping	No	No
Fault_Log_610	User-defined	User-defined

Important: If the `Environment Mapping`, `Relationships`, or `SVC_Port_Oper_Mapping` tables are pruned, the IBM Web Services Navigator is not able to correctly display service topology and transaction flows.

For information about estimating the size of these warehouse tables for historical data collection, see the section "Estimating table sizes in the Tivoli Data Warehouse for historical data collection " in the *IBM Tivoli Composite Application Manager for SOA User's Guide*.

Configuring historical data collection

Before configuring historical data collection, ensure that the warehouse database and warehouse proxy are configured and activated.

To configure historical data collection on ITCAM for SOA, complete the following steps:

1. Open and sign in to either the portal desktop or the portal browser.
2. In the TEP console, click the **History Collection Configuration** icon in the toolbar.

   The **History Collection Configuration** window displays.
3. In the **Monitored Applications** list, click the plus (+) sign to expand it, and select the ITCAM for SOA node.
4. Choose an attribute group. Only those attribute groups that are appropriate for historical collection and reporting are displayed.
5. Complete the following fields in the **Basic** tab:
   - Set the **Collection Internal**.

     This is the frequency with which the metric log files are collected by the monitoring agent and stored in a temporary location before they are sent to the warehouse database. The recommended value is 5 minutes. The ITCAM for SOA monitoring agent does not support a collection interval greater than 1 hour.
   - Leave the **Collection Location** selection at `TEMA` to have the log files collected at the Tivoli Enterprise Monitoring Agent for processing.
   - Set the **Warehouse Interval**.

     This is the frequency at which the metric log data is sent to the warehouse database for historical collection. You can select a frequency of once every hour or once per day. The recommended interval is once every hour.
   - Click **Apply**.
6. Complete the following steps on the **Distribution** tab to distribute the collection definition to the monitoring agent where you want to take data samples. Data collection begins as soon as you save the distribution:
   a. Click the **Managed System (Agent)** radio button to select managed systems and managed systems groups individually.

b. Move the ITCAM for SOA agent from the **Available Systems** list to the **Start Collection** list.

c. Click **Apply** to save your settings and start data collection.

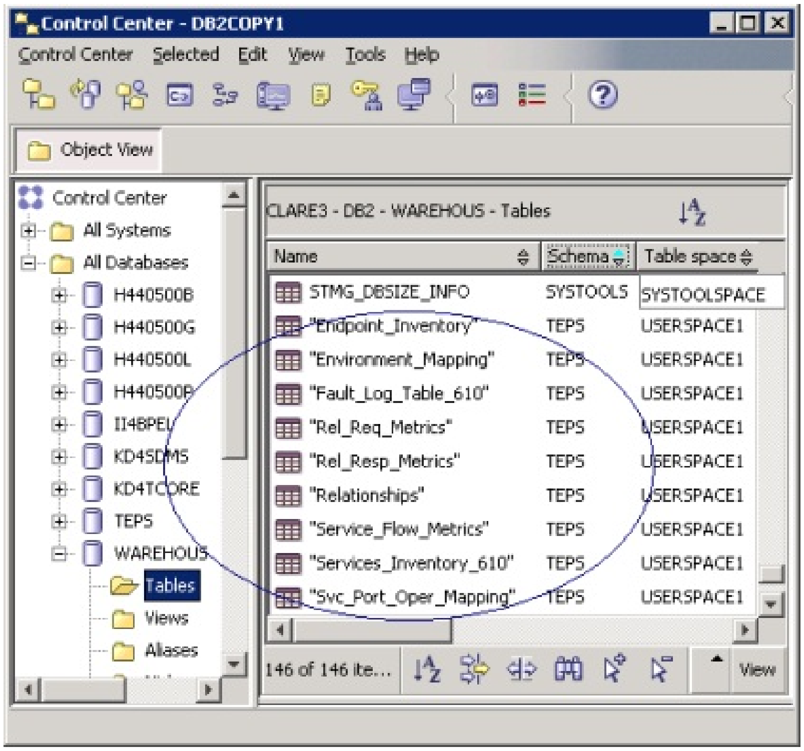
For information about assigning managed systems to a historical configuration group for the collection definition, see the I*BM Tivoli Monitoring: Tivoli Enterprise Portal User's Guide*.

Configuring summarization and pruning of attribute groups.

Configure summarization and pruning for the Tivoli Data Warehouse to aggregate data and keep the database size at a manageable level.

To configure summarization and pruning for ITCAM for SOA attribute groups, complete the following steps:

1. Open and sign in to either the portal desktop or the portal browser.
2. In the **Monitored Applications** list, choose ITCAM for SOA from the tree.
3. Click a row in the attribute groups table to configure an attribute group. Base your selections of attribute groups based on the recommendations provided in Table 61 on page 498.
4. In the Summarization area, select the check box for every time period to be aggregated: Yearly, Quarterly, Monthly, Weekly, Daily, and Hourly.
5. In the Pruning area, select the check box for every time period to be pruned: Yearly, Quarterly, Monthly, Weekly, Daily, and Hourly. If you also want to keep the original data samples, select the Detailed data check box. In the corresponding fields, specify the number of days, months, or years to keep the data.
6. Click **Apply** to save your settings.
7. After services data is written to the warehouse database for the first time (after approximately one hour or one day, depending on the **Warehouse Interval** value you specified), use your database software administrative tools to check the contents of the database tables. Verify that a table with the corresponding name for each configured attribute group is created in the database, as shown in the following DB2 example in Figure 75 on page 501 (DB2 is one of the warehouse databases types supported in Tivoli Monitoring).



Name	Schema	Table space
STMG_DBSIZE_INFO	SYSTOOLS	SYSTOOLSPACE
"Endpoint_Inventory"	TEPS	USERSPACE1
"Environment_Mapping"	TEPS	USERSPACE1
"Fault_Log_Table_610"	TEPS	USERSPACE1
"Rel_Req_Metrics"	TEPS	USERSPACE1
"Rel_Resp_Metrics"	TEPS	USERSPACE1
"Relationships"	TEPS	USERSPACE1
"Service_Flow_Metrics"	TEPS	USERSPACE1
"Services_Inventory_610"	TEPS	USERSPACE1
"Svc_Port_Oper_Mapping"	TEPS	USERSPACE1

Figure 75. ITCAM for SOA attribute group tables displayed in the DB2 Control Center

Chapter 20. Installing Discovery Library Adapters

After you install and configure support for SOA Domain Management Server and Tivoli Common Object Repository, you need to install one or more Discovery Library Adapters (DLAs) that populate the Tivoli Common Object Repository database with relationship information from WebSphere Service Registry and Repository (WSRR), from Business Process Execution Language (BPEL) information, and from services data obtained from the IBM Tivoli Composite Application Manager for SOA monitoring agents.

The following three DLAs are provided with ITCAM for SOA:

- WebSphere Service Registry and Repository DLA: Discovers the relationships between service ports, operations, services, port types, and metadata documents.
- Business Process Execution Language DLA: Discovers the relationships between port types, operations, and business processes.
- IBM Tivoli Composite Application Manager for SOA DLA: Discovers the relationships between service ports and operations and the application servers and computer systems on which they are deployed. The data is collected by the ITCAM for SOA monitoring agent and is retrieved from Tivoli Enterprise Monitoring Server.

The same versions of the DLAs are provided in ITCAM for SOA 7.2 and ITCAM for SOA 7.1.1. However, an additional WebSphere Service Registry and Repository DLA is provided in ITCAM for SOA version 7.2. If you want to discover services in WebSphere Service Registry and Repository version 8.0, you must install the WebSphere Service Registry and Repository DLA using the `WSRR8_DLA.bat` script.

If you want to discover services in WebSphere Service Registry and Repository version 8.5, you must update to ITCAM for SOA version 7.2 Fix Pack 1 Interim Fix 2 (7.2.0.1 IF2) or later and then install the WebSphere Service Registry and Repository DLA using the `WSRR85_DLA.bat` script.

There same versions of the DLAs are provided in ITCAM for SOA 7.2 Fix Pack 1 and ITCAM for SOA 7.2.

You install these DLAs from the ITCAM for SOA product installation media. For installation and configuration procedures and additional information about how to use the bulk load program to load the DLA information into the Tivoli Common Object Repository database, see the *IBM Tivoli Composite Application Manager for Discovery Library Adapters Guide*.

Chapter 21. Installing ITCAM for SOA Tools

The ITCAM for SOA tools incorporates the IBM Web Services Navigator.

Remember: Starting in version ITCAM for SOA version 7.2, managed SCA mediation primitives are no longer provided for insertion into mediation flow components of applications built with IBM WebSphere Integration Developer. The promotable properties of mediation primitives in IBM WebSphere Integration Developer provide a similar role.

The IBM Web Services Navigator is a plug-in that is based on Eclipse for extracting services information that is collected by the monitoring agents and stored either locally or in a historical database. The tool can retrieve historical metric data from a connected database, or assemble several locally stored metric and content log files, and display the resulting data in several views to assist services architects in visualizing relationships between services.

The installation of IBM Web Services Navigator involves running an Install Shield MultiPlatform (ISMP) installation program to install these tools on the preferred computer. You do not have to install the IBM Web Services Navigator on a computer where you are monitoring web services. You can install IBM Web Services Navigator on any computer in your environment that is running a supported operating system.

You install the IBM Web Services Navigator from the ITCAM for SOA product installation media. See the *IBM Tivoli Composite Application Manager for SOA Tools* guide for installation and configuration procedures.

Chapter 22. Installing ITCAM for SOA reports

ITCAM for SOA Reports is the reports package for ITCAM for SOA. You can use ITCAM for SOA Reports to create historical reports based on the data that is collected by ITCAM for SOA.

Tivoli Data Warehouse is the data source for ITCAM for SOA Reports. When you enable historical data collection for ITCAM for SOA, the collected data is stored in Tivoli Data Warehouse. A set of predefined reports is available with ITCAM for SOA Reports, but you can also create customized reports.

For detailed information about installing, configuring, and running ITCAM for SOA reports, see *IBM Tivoli Composite Application Manager for SOA Reports Guide*.

Chapter 23. Configuring Tivoli Monitoring to forward events

You can forward ITCAM for SOA situation events from the monitoring server to a Tivoli Enterprise Console® event server, to a Netcool® OMNIbus event server, or you can create one or more event destinations with the **tacmd createEventDest** command and configure individual situations to forward events to these destinations.

Forwarding events from the monitoring server to the Tivoli Enterprise Console

The ITCAM for SOA monitoring agent kd4.baroc and kd4.map files define the ITCAM for SOA events to forward to the Tivoli Enterprise Console event server. These files are available on the ITCAM for SOA installation media in the \kd4\tec directory on Windows and in the /kd4/tec directory on Linux and UNIX.

When you install application support files on the monitoring server, the kd4.baroc and kd4.map files are also copied to the following directory locations on the computer where monitoring server is installed:

- On Windows operating systems, the kd4.map and the kd4.baroc files are in the *ITM_Home*\CMS\TECLIB directory, where *ITM_Home* is the directory where you installed Tivoli Monitoring. For information about resolving directory path variables, see "Resolving directory path variables" on page xvi.
- On Linux and UNIX operating systems, the kd4.mapand the kd4.baroc files are in the *ITM_Home*/tables/*ms_name*/TECLIB directory, where *ms_name* is the name of the monitoring server.

The procedure for forwarding events from the monitoring server to the Tivoli Enterprise Console, including the procedure for installing .baroc files on the Tivoli Enterprise Console event server, are documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Forwarding events from the monitoring server to the Netcool/OMNIbus event server

You can also forward situation events from the monitoring server to an Netcool/OMNIbus event server. Events flow from the hub monitoring server to a Tivoli EIF probe. The EIF probe filters the events and forwards the events to a Netcool/OMNIbus ObjectServer.

The procedure for forwarding events from the monitoring server to the Netcool/OMNIbus event server is documented in the *IBM Tivoli: Installation and Setup Guide*.

Forwarding events to multiple event destinations

You can create event destinations for ITCAM for SOA situation events. In Tivoli Monitoring, you use the **tacmd createEventDest** command to create the event destination and the **tacmd refreshTECinfo** to trigger the Event Forwarded to reprocess the updated destinations. Using the Situation Editor on the portal server, you specify which situations to send to the event destinations.

The procedure for forwarding events to an event destination is documented in the *IBM Tivoli Monitoring: Administrators Guide*.

Event Integration with WebSphere Service Registry and Repository

ITCAM for SOA can be configured to subscribe to events from WebSphere Service Registry and Repository and to create, update, and delete situations based on the WebSphere Service Registry and Repository events it receives.

Using the Tivoli Monitoring Event Integration Facility (EIF), you can forward ITCAM for SOA events to WebSphere Service Registry and Repository when the situations for the WebSphere Service Registry and Repository profile trigger.

To forward situation events to WebSphere Service Registry and Repository, you must configure EIF event destinations in Tivoli Monitoring. In the WSRR SDMS configuration file, which defines how ITCAM for SOA processes WebSphere Service Registry and Repository notifications events, associate situations with event destinations. The WSRR SDMS configuration file is included in ITCAM for SOA version 7.2 Fix Pack 1. For information about integrating ITCAM for SOA with WebSphere Service Registry and Repository and about forwarding situation events to WebSphere Service Registry and Repository, see *IBM Tivoli Composite Application Manager for SOA WSRR Integration Guide*.

Chapter 24. Verifying the installation and configuration

After you have upgraded or installed ITCAM for SOA into your Tivoli Monitoring environment, configured for topology support, and enabled your runtime environments for monitoring and data collection by the ITCAM for SOA monitoring agent, complete these additional tasks, described in the sections that follow, to verify your installation and configuration.

1. Verify that the `KD4BaseDirConfig.properties` properties file was created successfully. See the section, "Verifying the properties file," for details.
2. Verify that the components of Tivoli Monitoring are started. See "Verifying Tivoli Monitoring components" on page 512 for details.
3. Stop and restart your application server services as needed.
4. The monitoring agent is automatically configured during installation. You can configure it again at any time by completing the steps in "Optional: Configuring the ITCAM for SOA monitoring agent" on page 512.
5. The monitoring agent is automatically started during the installation. See "Starting and stopping the monitoring agent" on page 513 for details on starting and stopping the monitoring agent.
6. Verify that metric log files are generated as expected when services traffic is monitored in your environment. See "Generating initial metric log files" on page 514 for details.
7. Start the Tivoli Enterprise Portal desktop client and verify that basic ITCAM for SOA workspaces are displayed. See "Verifying Tivoli Enterprise Portal workspaces" on page 516 for details.

Verifying the properties file

Check for a file named `KD4BaseDirConfig.properties` that is created automatically during the installation of ITCAM for SOA.

- For Windows operating systems, navigate to the %SYSTEMROOT%\system32\drivers\etc directory and verify that the file exists and has an entry similar to the following example:

  ```
  INSTALLDIR=C:\\IBM\\ITM\\TMAITM6\\
  ```

  This example assumes that Tivoli Monitoring is installed in the default directory, `C:\IBM\ITM`. If you installed to a different directory location, verify that this entry is correctly specified.
- For Linux, AIX, HP-UX, or Solaris operating systems, navigate to the `/etc` directory and verify that the file exists and contains an entry similar to the following examples:
  - For AIX operating systems:

    ```
    INSTALLDIR=/opt/IBM/ITM/aix523/d4
    ```
  - For HP-UX on RISC processors:

    ```
    INSTALLDIR=/opt/IBM/ITM/h11/d4
    ```
  - For HP-UX on Itanium processors:

    ```
    INSTALLDIR=/opt/IBM/ITM/hpi116/d4
    ```
  - For Linux:

    ```
    INSTALLDIR=/opt/IBM/ITM/li6263/d4
    ```
  - For Solaris:

```
INSTALLDIR=/opt/IBM/ITM/sol283/d4
```

- For zLinux:

```
INSTALLDIR=/opt/IBM/ITM/ls3263/d4
```

These examples assume that Tivoli Monitoring is installed in the default directory, */opt/IBM/ITM*. If you installed to a different directory location, verify that this entry is correctly specified. See "Resolving directory path variables" on page xvi to determine the correct platform designation.

The value in the `INSTALLDIR` variable represents the directory location where the `\KD4` directory is located. The `\KD4` directory contains logging and properties files used with ITCAM for SOA.

If the `KD4BaseDirConfig.properties` file does not already exist, the installation has likely failed to complete successfully. Check the installation log files and try the installation again. The file might not exist if you installed the monitoring agent using a non-root user on Linux or UNIX operating systems. In this case, you must manually copy the file from the *`ITM_Home/platform`*`/d4/KD4/config` directory to the `/etc` directory while logged in as a user with write access to the `/etc` directory.

Several properties files are created for controlling the configuration and behavior of the ITCAM Data Collector for WebSphere, if installed. The file `toolkit.properties` is created at startup and is unique for each application server instance being monitored. The file is located in the directory into which the ITCAM Data Collector for WebSphere is installed. For more information about the set of properties files and log files created for the ITCAM Data Collector for WebSphere, see "Properties files for the Data Collector" on page 321.

Verifying Tivoli Monitoring components

Open the Manage Tivoli Enterprise Monitoring Services utility and complete these steps:

1. Verify that the Tivoli Enterprise Monitoring Server is started.
2. Verify that the Tivoli Enterprise Portal Server is started.
3. If you plan to write services data to the data warehouse using the Warehouse Proxy, verify that the Warehouse Proxy is started.
4. Verify that the ITCAM for SOA agent is started.
5. Verify that the Eclipse Help Server, used to access the searchable online help files for the monitoring agent in the IBM Eclipse Help System, is started.

Optional: Configuring the ITCAM for SOA monitoring agent

After you have completed the documented procedures for installing and configuring the ITCAM for SOA monitoring agent, at a later time you might choose to modify the host name for the Tivoli Enterprise Monitoring Server. You can configure the monitoring agent again at any time by completing the following steps:

- For supported Windows operating systems:
  1. Right-click the **ITCAM for SOA** agent name and select **Reconfigure** to configure the agent.
  2. Follow any on-screen prompts to configure the agent for your environment. When completed, the icon to the left of the ITCAM for SOA entry turns to a green circle with a check mark, indicating the configuration completed successfully.

- For Linux and UNIX operating systems:
  1. Enter the following command:

     ```
     ./itmcmd config -A d4
     ```
  2. Press Enter when you are asked if the monitoring agent connects to a monitoring server.
  3. Type the hostname for the monitoring server.
  4. Type the type of protocol that the monitoring agent uses to communicate with the monitoring server. You have four choices: IP, SNA, IP.SPIPE, or IP.PIPE. Press Enter to accept the default protocol (IP.PIPE).
  5. If you want to set up a backup protocol, enter that protocol and press Enter. If you do not want to use backup protocol, press Enter without specifying a protocol. If the method you have identified as Protocol 1 fails, Protocol 2 is used. See the Tivoli Monitoring documentation for more information about available protocol selections.
  6. Depending on the types of protocols you specified, provide the information described in Table 62 when prompted:

Table 62. Linux, AIX, HP-UX, and Solaris Protocol settings for communicating between the monitoring agent and Tivoli Enterprise Monitoring Server

Protocol	Value	Description
IP	IP Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is *1918*.
IP.PIPE	IP.PIPE Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is *1918*.
IP.SPIPE	IP.SPIPE Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is *3660*.
SNA	Network Name	The SNA network identifier for your location.
	LU Name	The LU name for the Tivoli Enterprise Monitoring Server. This LU name corresponds to the local LU Alias in your SNA communications software.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is *CANCTDCS*.

  7. Press Enter to *not* specify the name of the KDC_PARTITION.
  8. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default response is *no*.
  9. Press Enter to accept the default for the Optional Primary Network Name (`none`).
  10. Continue with the next section, "Starting and stopping the monitoring agent."

Starting and stopping the monitoring agent

Start the agent from the Manage Tivoli Enterprise Monitoring Services utility by right-clicking the agent name, for example **ITCAM for SOA**, and selecting **Start** from the menu. Select **Stop** from the menu to stop the agent.

On supported Linux, AIX, HP-UX, or Solaris operating systems you can also start the monitoring agent by running the following command:

```
./itmcmd agent start product_code
```

For example:

```
./itmcmd agent start d4
```

Similarly, stop the agent by running this command:

```
./itmcmd agent stop product_code
```

For example:

```
./itmcmd agent stop d4
```

Starting the monitoring agent using a telnet session

If you use a telnet session to start the ITCAM for SOA monitoring agent from a Bourne shell, the monitoring agent might be unexpectedly terminated when you exit the telnet session. To avoid this potential problem in a telnet session, enter the Korn shell (ksh), and then start the monitoring agent.

Generating initial metric log files

Complete these steps to verify the initial generation of metric log files:

1. Optionally stop the operation of the **ITCAM for SOA** agent by right-clicking it in the Manage Tivoli Enterprise Monitoring Services console and selecting **Stop**.
2. Generate some initial appropriate services traffic for your application server runtime environment.
3. Navigate to the `ITCAM4SOA_Home\KD4\logs` directory and verify that a metric log file was created with a name similar in format to `KD4.field1.field2.field3.field4.field5.field6.metric.log`.

   Tip: In the metric log file name, `field6` is included in the name of some metric log files generated for IBM WebSphere Application Servers only.

   Where:

   ITCAM4SOA_Home
   is the location where the ITCAM for SOA monitoring agent is installed. For example:
   - On Windows: `C:\IBM\ITM\TMAITM6`
   - On Linux and UNIX: `/opt/IBM/ITM/platform/d4`, where *platform* is one of several values, depending on the operating system, the type of computer system, and version of IBM Tivoli Monitoring installed. See “Resolving directory path variables” on page xvi for the procedure to determine the value of *platform*.

   field1 Is an integer indicating the type of supported application server. Valid values include:
   - 1 = IBM WebSphere Application Server
   - 2 = Microsoft .Net
   - 3 = BEA WebLogic Server
   - 4 = JBoss
   - 5 = Customer Information Control System (CICS) Transaction Server
   - 6 = SAP NetWeaver
   - 7 = WebSphere Community Edition
   - 8 = DataPower SOA Appliance

- 10 = WebSphere Message Broker

field2 This is the name of the cluster containing the application server, and might be a null value (that is, an empty text string) if the application server is not part of a cluster (for example, in the DataPower environment, there is no concept of a cluster, so this field is not used).

field3 This is the name of the cell associated with the node for the application server, and might be a null value. For DataPower, this field contains the short hostname of the computer where the DataPower appliance is located.

field4 This is the node name, usually corresponding to a logical or physical computer system with a unique IP host address, where the application server is located, and serves as a logical grouping of one or more managed application servers. Typically this is identical to the hostname for the computer, and might be a null value. For DataPower, this field contains the name of the DataPower domain.

field5 This is the name of the application server (for example, server1 on WebSphere). For DataPower, this field contains the name of the DataPower display group. For certain default configurations, this display group name might be the same as the domain name or the appliance hostname.

field6 This field might be included in the metric file name if the application server type is IBM WebSphere Application Server. The field contains the type of IBM Business Process Manager (BPM) metric data generated in the file. The type can be set to `bpd`, `bpm`, or `bpm.static`. For example:

```
KD4.1.BPM_P7.AppTarget.testalp4Cell01.testalp5Node01.BPM_P7.AppTarget.
testalp5Node01.0.bpd.metric.log
KD4.1.BPM_P7.AppTarget.testalp4Cell01.testalp5Node01.BPM_P7.AppTarget.
testalp5Node01.0.bpm.metric.log
KD4.1.BPM_P7.AppTarget.testalp4Cell01.testalp5Node01.BPM_P7.AppTarget.
testalp5Node01.0.HTM_PredefinedTaskMsg_V7510_BPM_P7.
AppTarget.bpm.static.metric.log
```

If *field2*, *field3*, or *field4* names contain null values, the log file name will still include the separator period characters, for example, `kd4.`*`field1`*`....`*`field5`*`.metric.log`.

Examine the contents of this log file and verify that it contains expected metric information.

Remember: This log file is only present when the ITCAM for SOA monitoring agent is not started. When the monitoring agent is started, these metric log files are processed and stored in the directory named \KD4.DCA.CACHE.

4. If you have previously stopped the monitoring agent, start it again from the Manage Tivoli Enterprise Monitoring Services console. After a few seconds, examine the `\KD4\logs` directory again and notice that any metric log files have now been processed by the monitoring agent and have been moved into the `\KD4.DCA.CACHE` directory.

Verifying Tivoli Enterprise Portal workspaces

Do these steps to verify that the basic workspaces provided with ITCAM for SOA are displayed in the Tivoli Enterprise Portal as expected. You might need to refer to the online help and the *IBM Tivoli Composite Application Manager for SOA User's Guide* for information about navigating among the various workspaces, and for detailed descriptions of workspace nodes and other Tivoli Enterprise Portal features.

1. Sign in to the Tivoli Enterprise Portal:
   a. Open the Manage Tivoli Enterprise Monitoring Services console.
   b. From the console, double-click the Tivoli Enterprise Portal desktop client.
   c. Type your valid sign-in name (for example, the default user name `sysadmin`), and its valid password.

   After your credentials are validated, the Tivoli Enterprise Portal is displayed showing the default ITCAM for SOA workspaces and views.
2. View your generated services traffic:
   a. Expand the node tree in the Navigator Physical view in the upper-left portion of the workspace, selecting your desired operating system, computer system node, and the Services Management Agent node.
   b. Select the Services Management Agent Environment node or one of its data collector subnodes (if available) to view various bar charts of your services traffic (note that this node and its subnodes are not displayed in the view until after you run services traffic in your environment).
   c. If these charts show no data, generate some additional web traffic and wait approximately five minutes, then refresh the display to see your monitored metric data displayed in the views.

   Refresh your view automatically: You can configure the workspace to refresh automatically from the menu bar at the top of the workspace by selecting **View** > **Refresh Every** and then selecting your desired interval, from every 30 seconds to every 60 minutes.

If you configured SOA Domain Management Server support for topology data, complete these additional steps:

1. Assign topology views to your user name: If your user name has administrative authority, complete these steps:
   a. From the workspace menu bar, select **Edit** > **Administer Users**. The Administer Users configuration page is displayed.
   b. Highlight your user ID in the table.
   c. Click the **Navigator Views** tab.
   d. Under the **Available Views** section, locate the ITCAM for SOA Navigator View.
   e. Select this view and click the left arrow to move it under **Assigned Views** for your user ID.

   Your user name is now authorized to select the optional ITCAM for SOA topology views and workspaces. If you do not have administrative authority to add this capability, see your local administrator for assistance.
2. Display service-to-service topology workspaces and views: If your user name is configured to display ITCAM for SOA topology workspaces and views, complete these steps:
   a. If you have a large monitored environment with multiple application servers, you might want to navigate to a particular Services Management

Agent Environment node and then select an application server subnode in the Navigator Physical view, to limit the amount of topology data that is displayed in the topology workspaces and views. If you only have a single application server associated with a selected Services Management Agent Environment node, then select that node instead.

   b. Right-click the application server subnode (or the selected Services Management Agent Environment node) and select **Workspace** > **Operational Flow**.

   c. An Operational Flows for Application Server workspace is displayed, showing the relationship information collected from your services traffic for operation flows that invoke services for the selected application server runtime environment.

   d. Move your cursor over the various icons and connecting lines in the topology view to display additional flyover help text.

   e. Double-click an icon in the Operation Flow view to display more detailed information in the Interaction Details view of the workspace.

   Refer to the online help and the *IBM Tivoli Composite Application Manager for SOA User's Guide* for more information about viewing metric and topology data in these workspaces and views.

3. Display topology workspaces and views for service registry integration: If you configured the optional Tivoli Common Object Repository support for topology data, you can view service registry and business process integration topology workspaces and views by doing these steps:

   a. In the **View** field at the top of the Navigator Physical views, select the **ITCAM for SOA** Navigator logical view.

   b. Right-click the Services Management node, and select **Workspace** > **Services Management**.

   The Services Overview table view is displayed, but the table is empty until you use the Tivoli Common Object Repository bulk load program to populate the database with service registry and business process data from Discovery Library Adapter books. See Chapter 20, "Installing Discovery Library Adapters," on page 503 and the *IBM Tivoli Composite Application Manager for SOA User's Guide* for more information about Discovery Library Adapters.

Part 6. Appendixes

Appendix. Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully.

The accessibility features in the product enable users to:

- Use assistive technologies, such as screen reader software and digital speech synthesizers, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using the technology with this product.
- Perform tasks with the software using only the keyboard.

General Navigation

Each page has four main sections:

- Headerbar
- Toolbar
- Main tabs
- Content

Each page has navigation points for screen readers. The following navigation points are all H1:

- Title bar
- Main tabs
- Main form
- Section labels
- Table labels

Menu Navigation

You use the Go To menu at the top of the screen to navigate to any of the applications that you have access to. The Go To menu is a cascading menu that is three levels deep at its deepest point. The following instructions describe how to get started with JAWS:

1. To get to the Go To menu press Alt+G.
2. When you open the menu, JAWS reads the first application in the menu. If JAWS does not begin to read the entry, restart the screen reader.
3. Navigate the list of applications in the menus by using the arrow keys.
4. JAWS indicates if a menu item has submenus. To get to a submenu, press the right arrow or enter.
5. Press the left arrow to move up a level in the hierarchy. If you press the left arrow at the highest level of the Go To menu, you leave the menu completely.
6. Press the Enter key to enter an application.

Accessibility help

The Accessibility Help panels provide details on general navigation, menu navigation, and hot keys. Click **Accessibility Help** from the toolbar of the product to access the help panels.

Screen reader setting

The product contains a screen reader flag. When you turn on the screen reader flag, the user interface is optimized to work with JAWS for Windows®. You use the **User** tab in the Users application to turn on the screen reader flag.

Keyboard shortcuts

You can navigate within the applications by using a combination of keys.

Accessible reports

To use the accessibility tools to read reports, you must access the reports in Microsoft Excel. In the reports applications, select the **Run Reports** option in the **Select Action** menu. With this option, you can email an .xls file version of a report to yourself at a scheduled time.

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center. The IBM Human Ability and Accessibility Center is at the following web address: http://www.ibm.com/able

Index

A

accessibility xiv
activate application support 51
additional procedures 53
agent
  remote deployment 38, 231
aggregation 444
  across multiple domains 470
  all domains, single host, multiple users 470
  cluster of appliances 470
  DataPower 442, 468
  planning for 443
  using display group 468
appliance
  aggregating multiple, DataPower 442
  cluster, DataPower 470
  communicating with data collector 480
  DataPower 441
application domain
  DataPower 443
application server
  changing version 324, 325
  deleting profile 326
  restarting 352
  starting 353
  stopping 354
application server monitoring
  configuring 274, 299
    manually 329
  reconfiguring 284
  unconfiguring 282, 305
    manually 335
  upgrading 291, 294, 308, 312
application support
  overview 10
asynchronous flows
  in SCA 257
authentication
  SOA Domain Management Server 163, 217
    authentication 163
  Tivoli Common Object Repository 218
    authentication 218
AXIS2 implementation
  JAX-WS support 257

B

background mode
  DataPower data collector 474
baroc file, kd4.baroc 509
BEA WebLogic Server 19, 84
  enabling applications for data collection 399
books
  see publications xi, xiii
BPC Explorer link 319
bulk load program, DLA 503
Business Process Monitoring 258

C

Client properties files 323
  sas.client.props file 323
  soap.client.props file 324
cluster
  DataPower SOA appliances 470
configuration file
  DataPower 442, 459
configuration items 49
configuring
  forward events 509
configuring application server monitoring 274, 299
  manually 329
configuring data collector 274, 299
  manually 329
configuring, data collection 375
conventions
  operating system xv
  typeface xv
cookies 528
copying files 48

D

data collection
  disabling WebSphere Message Broker applications for 360, 369
  enabling BEA WebLogic Server applications for 399
  enabling IBM CICS Transaction Server applications for 415
  enabling JBoss applications for 409
  enabling Microsoft .Net applications for 397
  enabling SAP NetWeaver applications for 417
  enabling WebSphere Application Server applications for 257
  enabling WebSphere Message Broker applications for 365
  permissions 376
data collection, configuring 375
data collector
  communicating with appliance 480
  configuring 274, 299
    manually 329
  configuring in DataPower environment 459
  considerations 17
  Data Collector for WebSphere Message Broker 7
  DataPower 441
  DataPower,
    upgrading 25, 30
  DataPower, deploying 444
data collector *(continued)*
  DataPower, starting 474
  DataPower, stopping 474
  DataPower, unconfiguring 445
  disabling 351
  disabling for DataPower 473
  disabling JBoss applications for 412, 413
  disabling SAP NetWeaver application for 426
  disabling WebSphere CE applications for 438
  enabling WebSphere CE applications for 431
  ITCAM Data Collector for WebSphere 7
  ITCAM for SOA 6
  reconfiguring 284
  remote deployment enabling 72, 106
  unconfiguring 282, 305
    manually 335
  upgrading 291, 294, 308, 312
  WebSphere Community Edition (CE) 431
  WebSphere Message Broker,
    updating 30
    upgrading 25
Data Collector Configuration utility 53, 375
data collector properties 321
data collector,
  disabling 25, 30
Databases
  overview 13
datacollector_custom.properties 321
datacollector.properties 321
DataPower 84, 441
  appliance, cluster 470
  appliance, configuring 445
  appliance, polling 442
  configuration file 459
  configuring environment for the data collector 459
  Console user interface in TEP 487
  data collector, background mode 474
  data collector, starting and stopping 474
  disabling data collector 473
  firmware upgrade 442, 445
  logging in 488
  multiple connections 468
  proxy 442
  style sheets 454
  user account, configuring 445
  user password 467
DataPower Console
  considerations 488
DB2 41, 83
deployment depot 38, 63, 97, 231, 251
destination folder 42
directory names, notation xv

disabling data collectors 351
Discovery Library Adapter 503
Discovery Library Adapters
  overview 12
display group
  aggregation and separation 468
  changing current value 467
  DataPower 444
displaygroup
  in node name, DataPower 465
DLA
  See also Discovery Library Adapter
  bulk load program 503
domain
  aggregating multiple, DataPower 442
  application, DataPower 443
domain list
  changing current value 467
  restricting user access 468
duplicate server instances, removing 317

E

Eclipse
  Help Server 41, 83, 232, 243
education
  see Tivoli technical training xiv
enabling
  application support 36, 230
    Linux and UNIX systems 239
encryption key for your ITCAM for SOA environment, defining 43
environment variables, notation xv

F

filtering
  SCA 319
firmware
  DataPower requirement 445
  DataPower requirements 442

G

glossary xiii

H

heap size 326
historical data collection 497
host
  in node name, Datapower 465

I

IBM CICS Transaction Server
  enabling applications for data collection 415
IBM Support Assistant
  contacting xiv
IBM Web Services Navigator
  overview 12
Installation roadmap 20
installation, planning for 3
installing
  application support
    Linux and UNIX systems 77, 78, 240
  ITCAM Data Collector for WebSphere 261
  Linux or UNIX systems 77, 238
  monitoring agent 37, 230
  Windows systems 35, 229
installing language support 75, 108, 238, 250
installing,
  installing 55
  ITCAM Data Collector for WebSphere 55
  monitoring agent 40, 81, 84
  planning for 19
  prerequisites 19
installing, Tivoli Monitoring 20
integrating 272
integrating,
  WebSphere Message Broker data collector 368
IP address 325
ITCAM Data Collector for WebSphere
  remote deployment 66, 69, 100, 103
ITCAM for SOA SDMS agent
  overview 229
ITCAM for SOA SDMS agent, configuring
    Linux and UNIX systems 246
ITCAM for SOA Tools
  overview 12
ITCAM for Transactions 272, 489
  integrating with DataPower appliance 489
  integrating with Microsoft .NET 489
itmcmd, agent start, stop 513
itmcmd, config 93, 244

J

JAX-RPC
  JBoss 409
JAX-WS support 257
JBoss
  disabling applications for data collector 412, 413
  enabling applications for data collection 409

K

kd4.baroc 509
kd4.map 509
KD4BaseDirConfig.properties 511
KD4configDC 375
  See also Data Collector Configuration Utility
  DataPower, optional parameters 468
  for BEA WebLogic Server 399
  for DataPower 463
  for IBM CICS Transaction Server 415
  for JBoss 409
  for Microsoft .Net 397
  for SAP NetWeaver 417, 424, 427
KD4configDC *(continued)*
  for WebSphere CE 432, 439
  parameters, DataPower 463
  running 392
KD4LN0001E error message 488
KD4LN0002E error message 488
knowledge base
  searching xiv

L

language pack,
  installing 75, 108, 238, 250
language packs
  uninstalling 75
license agreement, product 42
limitations
  DataPower 482
logging
  DataPower 483
  SCA 319

M

managed system list 52
manual configuration 329
manual unconfiguration 335
manuals
  see publications xi, xiii
mediation 257
Microsoft .Net
  enabling applications for data collection 397
Microsoft SQL Server 41
monitoring agent
  installing 40, 81, 84
  remote deployment 46, 63, 65, 69, 97, 99, 102, 251, 253
  silent installation 61, 95, 235, 247
  upgrading 40, 81, 84
Monitoring agent
  overview 5
monitoring agent,
  changing file permissions 94
  configuring 58
    Linux and UNIX systems 93, 244
monitoring agent, starting and stopping 513
Multi-Protocol Gateway
  DataPower 441
multiple connections
  DataPower 468

N

NetWeaver
  see SAP NetWeaver 417
node name
  in TEP, for DataPower 465
notation
  environment variables xv
  path names xv
  typeface xv

O

online publications
  accessing xiii
Oracle 41, 83
ordering publications xiii
overview 3, 23, 28

P

parameters
  KD4configDC for DataPower, optional 468
password
  DataPower, specifying 467
path names, notation xv
performance
  DataPower 481
Performance Summary workspace 487
permission,
  monitoring agent 35, 229
permission, monitoring agent 94
permissions
  ITCAM Data Collector for WebSphere 273
permissions,
  monitoring agent
    Linux and UNIX systems 83, 239
planning 3
platform code 93
poll
  DataPower SOA appliance 442
portal server host name 51
prerequisites
  hardware 15
  software 15
privacy policy 528
problem determination
  guidance xiv
processing rules
  configuring, for DataPower 447
properties files 321
proxy
  DataPower 442
publications
  accessing online xiii
  feedback xi
  online xi
  ordering xi, xiii

R

rebuilding the portal server
  Linux and UNIX systems 227
reconfiguring application server monitoring 284
reconfiguring data collector 284
reconfiguring the portal server 173
remote agent deployment 38, 231
remote deployment
  data collector
    enabling 72, 106
  ITCAM Data Collector for WebSphere
    command prompt 66, 100
    migrating 69, 103
  monitoring agent 63, 97, 251
    command prompt 65, 99, 253

remote deployment *(continued)*
  monitoring agent *(continued)*
    Tivoli Enterprise Portal 64, 98, 253
    upgrading 69, 102
removing the product 72, 106
report request limit 172
  Linux and UNIX systems 226
requester identity,
  configuring 479, 480
restarting application servers 352
restoring configuration 327
Roadmap,
  installation 20
  updating 30
  upgrading 26
root user 326

S

SAP 417
SAP NetWeaver
  disabling application for the data collector 426
  enabling applications for data collection 417
SCA
  components 257
  filtering 319
  limitations 317
  logging 319
  modules 257
Self-describing agent
  Linux and UNIX systems 77, 239
  Windows 36, 230
SELinux 92
separation
  between domains by domain list 469
  by display group 469
  by host name 469
  DataPower 468
  using display group 468
service xiv
service management connect xiv
Services Inventory attributes table 487
silent installation,
  monitoring agent 61, 95, 235, 247
SMC xiv
SOA Domain Management Server 13, 111
  authentication 217
  DB2 database
    Linux and UNIX systems 185, 187
    Windows 121, 124
  Linux and UNIX systems 175
  Microsoft SQL Server database
    Windows 122, 125
  Oracle database
    Linux and UNIX systems 185, 188
    Windows 123, 126
  overview 11
SOA Domain Management Server Configuration
  configuring 148, 208

SOA Domain Management Server Configuration *(continued)*
    SOA Domain Management Server Configuration 148, 208
SOA Domain Management Server Configuration utility 132, 137
  Linux and UNIX systems 194, 198
start monitoring agent 513
startDC 474, 480
  starting DataPower data collector 444
starting
  application servers 353
stop monitoring agent 513
stopDC 474
  stopping DataPower data collector 445
stopping
  application servers 354
support xiv
  obtaining xiv
  online xiv
synchronous flows
  in SCA 257

T

telnet, starting from 513
terminology xiii
Tivoli Common Object Repository 14, 111
  configuring 157, 213
    Tivoli Common Object Repository 157, 213
  DB2 database
    Linux and UNIX systems 190, 192
    Windows 128, 130
  Linux and UNIX systems 175
  Oracle database
    Linux and UNIX systems 190, 193
    Windows 129, 131
  overview 11
Tivoli Common Reporting 507
Tivoli Data Warehouse 13
Tivoli Enterprise Portal
  display group, DataPower 444
  node names, DataPower 465
Tivoli Monitoring 3
  overview 4
Tivoli software information center xiii
Tivoli technical training xiv
Tivoli user groups xiv
toolkit properties 321
toolkit_custom.properties 321
toolkit_global_custom.properties 321
toolkit.properties 321
topology support, permissions
  Linux and UNIX 178
  Windows 115
topology support, planning
  Linux and UNIX 178
  Windows 114
tracing
  DataPower 483
training, Tivoli technical xiv

transaction log service
  DataPower 442
troubleshooting 482, 484
  appliance password 483
  communication 483
  synchronizing time 483
typeface conventions xv

U

unconfiguring application server monitoring 282, 305
  manually 335
unconfiguring data collector 282, 305
  manually 335
uninstall
  on Linux and UNIX systems 250
  on Linux, AIX, HP-UX, Solaris 107
uninstalling 72, 106
  ITCAM for SOA 72, 106
  language packs 75
update roadmap 30
updateLogging Take Action 480
updating
  topology support 134
Updating
  ITCAM Data Collector for WebSphere 272
updating, 28
  Linux and UNIX systems 196
  planning for 29
  topology support 196
upgrade roadmap 26
upgrading
  ITCAM Data Collector for WebSphere 266
  Linux or UNIX systems 77, 238
  Windows systems 35
upgrading application server monitoring 291, 294, 308, 312
upgrading data collector 291, 294, 308, 312
upgrading, 23
  Linux and UNIX systems 195
  monitoring agent 40, 81, 84
  planning for 24
  topology support 133, 195
upgrading, Tivoli Monitoring 25
User Account Control 39
user groups, Tivoli xiv

V

variables, notation for xv

W

Web Services Navigator 505
web services proxy
  DataPower 441
WebSphere Application Server
  enabling applications for data collection 257
WebSphere CE 431
  disabling applications for data collector 438
WebSphere CE *(continued)*
  disabling applications manually 440
  enabling applications manually 435
  enabling for the data collector 431
WebSphere Community Edition 431
WebSphere Message Broker
  disabling applications for data collection 360, 369
  enabling applications for data collection 365

X

XML Management Interface
  enabling, for DataPower 446

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s user name for purposes of session management, authentication, and single sign-on configuration. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Printed in USA

GC23-8803-05