Note!

Before using this information and the product it supports, read the information in Appendix H, "Notices," on page 257.

This edition of the Installation and Configuration Guide applies to Version 2, Release 3, Modification 0 of IBM Tivoli System Automation for Multiplatforms, program number 5724-M00, and to all subsequent releases and modifications of this product until otherwise indicated in new editions.

IBM welcomes your comments. A form for readers’ comments may be provided at the back of this publication, or you may address your comments to the following address:

IBM Deutschland Entwicklung GmbH
Department 3248
Schoenaicher Str. 220
D-71032 Boeblingen
Federal Republic of Germany

FAX (Germany): 07031+16-3456
FAX (Other Countries): (+49)+7031-16-3456

Internet e-mail: eservdoc@de.ibm.com

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

• Title and order number of this book
• Page number or topic related to your comment

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

© Copyright International Business Machines Corporation 2006, 2007. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Contents

Figures ........................................ vii
Tables .......................................... ix

About this guide ................................ xi
Who should read this guide ...................... xi
How to use this guide .......................... xi
Where to find more information ............... xi
Conventions used in this guide ................ xii
Typeface conventions .......................... xii
Related information ............................ xii

Summary of changes ............................ xv
What's new in release 2.3 ...................... xv

Part 1. Base component and SA operations console .................... 1

Chapter 1. Installing the Base component for AIX and Linux .......... 3
Planning for the installation .................. 3
Coexistence with other products ............... 3
Contents of the CD ............................. 3
CDs / archives for the Base component ...... 3
Electronic distribution of IBM Tivoli System Automation ............... 4
Supported platforms ........................... 4
Supported network interfaces .................. 5
Preparing for installation ...................... 6
Prerequisites ................................. 6
Initial configurations ......................... 7
Installing and upgrading the Base component .............. 9
Installing the Base component for AIX and Linux 9
Installing the product license ................ 11
Upgrading from a Try & Buy license to a full product license .......... 11
Languages and locales supported by the Base component .......... 11
Migrating the Base component ............... 12

Chapter 2. Installing the Base component operations console ......... 17
Planning for the installation .................. 17
Packaging ............................. 17
Product requirements ........................ 19
Preparing for the installation of the Base component operations console 21
Collecting the information you need to provide during installation 21
Installation prerequisites ..................... 25
Installing the Base component operations console using the graphical installation program 26
Installing the Base component operations console in silent mode ........... 33
Verifying the installation .................. 33

Chapter 3. Upgrading the operations console from release 2.2 ....... 37

Chapter 4. Configuring the operations console ......................... 39
Configuring the end-to-end automation adapter to use the operations console 39
Configuring the operations console for direct access mode ............. 39
Planning the configuration ................... 39
Using the configuration dialog ............... 39

Chapter 5. Uninstalling the Base component for AIX and Linux and the operations console ......................... 41
Uninstalling the Base component for AIX and Linux 41
Uninstalling the Base component operations console .............. 42
Launching the graphical uninstallation program on Windows .......... 42
Launching the graphical uninstallation program on AIX and Linux ...... 42
Using the uninstallation program ............... 42

Chapter 6. Installing the Base component for Windows .............. 47
Planning for the installation .................. 47
Base component installation CD ............... 47
Base component installation archive .......... 47
Supported languages and locales ............ 47
Preparing the system for the installation of the Base component for Windows .............. 47
Installation prerequisites ..................... 47
Installing the Subsystem for UNIX-based Applications (required) ........ 48
Installing the Utilities and SDK Package (required) ................. 48
Ensuring that the Administrator UID is set to the correct value .......... 49
Verifying the directory structure (required) .................. 49
Verifying and updating TCP/IP configuration files (required) .......... 49
Upgrading the DNS or hosts file (required) .................. 49
Configuring the Subsystem for UNIX-based Applications ............... 50
Installing the Base component for Windows ............... 52
Verifying the installation ................... 52
Default profile changes made to your default profile .......... 59
License installation .......................... 60
Setting up the Windows firewall ............... 60
Figures

1. Verifying the active and installed version numbers ........................................ 14
2. Log in panel of Integrated Solutions Console ................................................. 34
3. Welcome panel of Integrated Solutions Console .............................................. 35
4. Setup of the End-to-End Automation Management component .......................... 79
5. Log in panel of Integrated Solutions Console ................................................ 113
6. Welcome panel of Integrated Solutions Console .............................................. 113
7. Configuration dialog task launcher .................................................................. 120
8. Domain tab ...................................................................................................... 122
9. Overview of the environment the end-to-end automation adapter works on ........ 160
10. Main panel of the end-to-end automation adapter configuration dialog ............ 162
11. System Automation for Multiplatforms end-to-end adapter configuration .......... 163
12. Host using adapter tab .................................................................................. 165
13. Automating the adapter .................................................................................. 167
14. Configuring the adapter security ................................................................... 170
15. Adapter logging and trace information ............................................................ 172
16. Configuration update status panel ................................................................. 174
17. System Automation for Multiplatforms replicate configuration files panel ......... 175
18. Configuration alternatives for the HACMP adapter ......................................... 181
19. Main panel of the HACMP adapter configuration dialog .................................. 182
20. Adapter tab of the HACMP adapter configuration dialog .................................. 183
21. Host using adapter tab of the HACMP configuration dialog ............................ 185
22. Automation tab of the HACMP configuration dialog ........................................ 186
23. Security tab of the HACMP configuration dialog ............................................ 188
24. HACMP configuration dialog: Logger tab ...................................................... 189
25. Configuration update status panel of the HACMP configuration dialog ............ 192
26. Replicate configuration files panel of the HACMP adapter configuration dialog 192
27. Adapter tab of the MSCS adapter configuration dialog .................................... 203
28. Configuration alternatives for the VCS adapter .............................................. 219
29. Main panel of the VCS adapter configuration dialog ........................................ 220
30. Adapter tab of the VCS adapter configuration dialog ....................................... 221
31. Host using adapter tab of the VCS configuration dialog ................................... 223
32. Automation tab of the VCS configuration dialog ............................................. 224
33. Security tab of the VCS configuration dialog ................................................ 226
34. VCS configuration dialog: Logger tab ............................................................. 227
35. Configuration update status panel of the VCS configuration dialog ................ 230
36. Replicate configuration files panel of the VCS adapter configuration dialog ..... 230
# Tables

1. Product CD versions .................................................. 4
2. Archives for Linux platforms ......................................... 4
3. Archives for AIX platforms ........................................... 4
4. Supported platforms for the Base component of IBM Tivoli System Automation for Multiplatforms .......................... 5
5. Software packages available for installation, based on your operating system .................................................. 6
6. Languages and locales supported by the Base component on Linux systems ...................................................... 12
7. Languages and locales supported by the Base component on AIX systems .......................................................... 12
8. Product CD versions ..................................................... 17
9. Archives for Windows platforms ....................................... 18
10. Archives for AIX platforms ............................................ 18
11. Archives for Linux on System x ....................................... 18
12. Archives for Linux on POWER ......................................... 18
13. Archives for Linux on System z ....................................... 19
14. Supported operating systems ........................................... 19
15. Disk space requirements for the installation on Windows systems ................................................................. 21
16. Disk space requirements on AIX and Linux systems ................. 21
17. Installation directory and Tivoli Common Directory .................. 22
18. Installation parameters for Integrated Solutions Console ......... 24
19. Port assignment for the embedded version of IBM WebSphere Application Server .............................................. 25
20. Languages and locales supported by the Base component for Windows .......................................................... 47
21. Windows firewall: Required port exceptions .......................... 60
22. IBM Tivoli System Automation Shell properties ..................... 61
23. Windows command prompt properties ................................... 62
24. Telnet session properties .................................................. 62
25. Session properties ......................................................... 62
26. Session properties ......................................................... 62
27. Archive for Linux platforms ............................................. 68
28. Archive for AIX platforms ............................................... 68
29. Archive for Windows platforms ......................................... 68
30. Windows platforms ....................................................... 70
31. AIX platforms ............................................................. 70
32. Linux on IBM System x ................................................... 70
33. Linux on POWER .......................................................... 70
34. Linux on System z ........................................................ 71
35. Product CD versions ...................................................... 75
36. WebSphere Application Server upgrade CD versions ............... 76
37. Archives for Windows platforms ....................................... 76
38. Archives for AIX platforms ............................................. 77
39. Archives for Linux on System x ....................................... 77
40. Archives for Linux on POWER .......................................... 77
41. Archives for Linux on System z ....................................... 78
42. Supported operating systems ............................................ 80
43. Disk space requirements on Windows systems ....................... 82
44. Disk space requirements on AIX and Linux systems ................. 83
45. Contents of the WebSphere Application Server 6.1.0 upgrade CD ................................................................. 88
46. Installation directory and Tivoli Common Directory ................. 90
47. DB2 data for local and remote DB2 setup ............................. 92
48. WebSphere Application Server installation parameters .............. 93
49. Installation parameters for IBM Tivoli Enterprise Console ......... 94
50. Name of the end-to-end automation domain .......................... 94
51. Name of the end-to-end automation domain .......................... 94
52. Directories on the product CD .......................................... 95
53. Languages and locales supported by End-to-End Automation Management component on Linux systems ................ 96
54. Languages and locales supported by the End-to-End Automation Management component on AIX systems ............... 96
55. Resources in the automation policy for the end-to-end automation manager ...................................................... 136

© Copyright IBM Corp. 2006, 2007
<table>
<thead>
<tr>
<th></th>
<th>56. Windows platforms</th>
<th>140</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>57. AIX platforms</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>58. Linux on System x</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>59. Linux on POWER</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>60. Linux on System z</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>61. Context used to find a Tivoli Enterprise Portal workspace</td>
<td>153</td>
</tr>
<tr>
<td></td>
<td>62. Resources in the end-to-end automation adapter policy</td>
<td>176</td>
</tr>
<tr>
<td></td>
<td>63. End-to-end automation adapter command options</td>
<td>177</td>
</tr>
<tr>
<td></td>
<td>64. Resources in the HACMP adapter automation policy</td>
<td>193</td>
</tr>
<tr>
<td></td>
<td>65. HACMP adapter command options</td>
<td>194</td>
</tr>
<tr>
<td></td>
<td>66. Resources in the VCS adapter automation policy</td>
<td>231</td>
</tr>
<tr>
<td></td>
<td>67. VCS adapter control command options</td>
<td>232</td>
</tr>
</tbody>
</table>
About this guide

This guide provides information needed to plan, install, configure, and upgrade IBM Tivoli System Automation for Multiplatforms.

Who should read this guide

This guide is for planners, installers, and administrators who plan to install and configure IBM Tivoli System Automation for Multiplatforms.

How to use this guide

This guide is divided into the following parts:

- **Part 1, “Base component and SA operations console,” on page 1** describes how to install, uninstall, service, and configure the Base component and the Base component operations console.
- **Part 2, “End-to-End Automation Management component,” on page 73** describes how to install, uninstall, service, and configure the End-to-End Automation Management component.
- **Part 3, “Enabling launch-in-context support,” on page 147** describes how you install and configure the IBM TEC extension for Tivoli System Automation for Multiplatforms, which enables users to navigate from an event displayed in the Event Console of Tivoli Enterprise Console to the corresponding resource or domain in the SA operations console, and describes how to set up launch-in-context support for Tivoli Enterprise Portal TEP), which enables users to launch TEP workspaces from the SA operations console with a single mouse click.
- **Part 4, “Installing and configuring the end-to-end automation adapters,” on page 155** describes how to install and configure the HACMP™, MSCS, and VCS adapters and the end-to-end automation adapter of the Base component for AIX and Linux.
- The Appendixes provide troubleshooting information.

Where to find more information

In addition to this manual, the IBM Tivoli System Automation for Multiplatforms library contains the following books:

- **IBM Tivoli System Automation for Multiplatforms Base Component Administrator’s and User’s Guide**, SC33-8272
- **IBM Tivoli System Automation for Multiplatforms Base Component Reference**, SC33-8274
- **IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Reference**, SC33-8276

You can download the complete documentation at

The IBM Tivoli System Automation for Multiplatforms home page contains useful up-to-date information, including support links and downloads for maintenance packages.

You find the IBM Tivoli System Automation for Multiplatforms home page at:


---

**Conventions used in this guide**

This guide uses several conventions for special terms and actions and operating system commands and paths.

**Typeface conventions**

This guide uses the following conventions:

- Typically, file names, directories, and commands appear in a different font. For example:
  - File name: setup.jar
  - Directory: /etc
  - Command: startServer server1
- Variables are either italicized, enclosed in brackets, or both. For example:
  - http://<hostname.yourco.com>/index.html
- Frequently, variables are used to indicate a root installation directory:
  - Root installation directory of the End-to-End Automation Management component:
    <EEZ_INSTALL_ROOT> or EEZ_INSTALL_ROOT
  - WebSphere Application Server root installation directory: <was_root> or was_root
- Directories are shown with forward slashes (/), unless operating-system specific information is provided. On Windows® systems, you should use backward slashes (\) when typing at a command line, unless otherwise noted.
- Operating-system specific information is provided. For example:
  - AIX, Linux: /opt/IBM/tsamp/eez
  - Windows: C:\Program Files\IBM\tsamp\eez

---

**Related information**

This topic provides information about publications and Web sites related to IBM Tivoli System Automation for Multiplatforms:

**WebSphere Application Server publications:**

The latest versions of all WebSphere Application Server publications can be found on the WebSphere Application Server library Web site at

[www.ibm.com/software/webservers/appserv/was/library/](http://www.ibm.com/software/webservers/appserv/was/library/)

**IBM Reliable Scalable Cluster Technology (RSCT) documentation:**

- The following RSCT publications are available on the IBM Tivoli System Automation for Multiplatforms Base component CD:
  - RSCT Administration Guide, SA22-7889
  - RSCT for AIX 5L: Technical Reference, SA22-7890
  - RSCT for Linux: Technical Reference, SA22-7893
- RSCT Messages, GA22-7891
- RSCT Diagnosis Guide, SA23-2202

* RSCT publications can also be found at the following Web site:
  www.ibm.com/servers/eserver/clusters/library/

**IBM DB2 publications:**
DB2 publications can be found on the IBM DB2 UDB Web site at
www.ibm.com/software/data/db2/udb/support/

The link to the PDF manuals is available in the Other resources section on the Web page.

**IBM Redbooks publications:**
The following publication are available at:
www.redbooks.ibm.com/redbooks.nsf/
- Linux on IBM zSeries and S/390: High Availability for z/VM and Linux
- End-to-End Automation with IBM Tivoli System Automation for Multiplatforms (SG24-7117-00)
Summary of changes

What's new in release 2.3

The following new features and enhancements are provided in Version 2 Release 3:

Automation adapter for VERITAS Cluster Server (VCS) clusters (VCS adapter)
The VCS adapter allows you to manage Sun Solaris/SPARC clusters that are made highly available with VCS as first-level automation domains. The installation and configuration of the adapter is described in Chapter 21, "Installing and configuring the VERITAS Cluster Server adapter," on page 217.

High availability for the End-to-End Automation Management component can be provided
You can use the Base component to provide high availability for the End-to-End Automation Management component. To configure high availability, you use the end-to-end automation manager configuration dialogs (see "Configuring high availability for the end-to-end automation manager" on page 128).

The Base component is also available for Windows Server 2003 systems
The Base component is also available for Windows Server 2003 R2. It makes use of the "Subsystem for Unix-based Applications" (SUA) from Microsoft which must be separately installed from the Windows Server 2003 installation media. For more information, see Chapter 6, "Installing the Base component for Windows," on page 47.

IBM TEC extension for launch-in-context is available
The IBM TEC Extension for Tivoli System Automation for Multiplatforms allows navigating from a displayed event in the Event Console of Tivoli Enterprise Console (TEC Event Console) to the corresponding resource or domain in the SA operations console. The installation of the TEC Extension is described in Chapter 15, "Installing and configuring the IBM TEC Extension for Tivoli System Automation for Multiplatforms," on page 149.

TEP launch-in-context support is available
If Tivoli Enterprise Portal (TEP) for resource monitoring and management is used, the launch-in-context support for Tivoli Enterprise Portal can be set up. Launch-in-context support enables users to launch Tivoli Enterprise Portal workspaces from the SA operations console with a single mouse click. The setup the TEP launch-in-context support is described in Chapter 16, "Setting up Tivoli Enterprise Portal launch-in-context support," on page 153.
Part 1. Base component and SA operations console

Chapter 1. Installing the Base component for AIX and Linux ............................. 3
Planning for the installation .................................................. 3
Coexistence with other products ............................................. 3
Contents of the CD ............................................................ 3
CDs / archives for the Base component .................................... 3
Base component CD .......................................................... 3
Electronic distribution of IBM Tivoli System Automation .................. 4
Archives ............................................................................ 4
Supported platforms ............................................................ 4
Supported network interfaces .................................................. 5
Preparing for installation ....................................................... 6
Prerequisites ....................................................................... 6
Initial configurations ........................................................... 7
Installing and upgrading the Base component .............................. 9
Installing the Base component for AIX and Linux ....................... 9
Performing the prerequisites check ........................................... 9
Installing the Base component ............................................... 9
Post-installation task ........................................................... 10
Installing the product license .................................................. 11
Upgrading from a Try & Buy license to a full product license .......... 11
Languages and locales supported by the Base component ............ 11
Base component for Linux ...................................................... 11
Base component for AIX ....................................................... 12
Migrating the Base component ................................................. 12
Migrating an entire domain .................................................... 13
Performing a node-by-node migration ..................................... 13
Verifying the active and installed version number ....................... 14
Completing the migration ....................................................... 15

Chapter 2. Installing the Base component operations console ....................... 17
Planning for the installation ................................................... 17
Packaging .......................................................................... 17
Operations console CD ......................................................... 17
Electronic distribution .......................................................... 17
Product requirements ........................................................... 19
Supported platforms ............................................................ 19
Supported Web browsers ....................................................... 20
Hardware requirements ........................................................ 20
Preparing for the installation of the Base component operations console ......................................................... 21
Collecting the information you need to provide during installation ......................................................... 21
Installation directory and Tivoli Common Directory .................. 21
Installation parameters for the Base component operations console ............................................................. 23
Port assignment for the embedded version of IBM WebSphere Application Server ....................................... 24
Installation prerequisites ........................................................ 25
Installing the Base component operations console
using the graphical installation program .................................. 26
Installing the Base component operations console in silent mode ......................................................... 33
Verifying the installation ....................................................... 33

Chapter 3. Upgrading the operations console from release 2.2 ......................... 37

Chapter 4. Configuring the operations console .............................................. 39
Configuring the end-to-end automation adapter to use the operations console ........................................ 39
Configuring the operations console for direct access mode .......... 39
Planning the configuration ..................................................... 39
Using the configuration dialog ................................................. 39

Chapter 5. Uninstalling the Base component for AIX and Linux and the operations console ................................................................. 41
Uninstalling the Base component for AIX and Linux .................. 41
Uninstalling the Base component operations console ................ 42
Launching the graphical uninstallation program on Windows ........ 42
Launching the graphical uninstallation program on AIX and Linux ......................................................... 42
Using the uninstallation program ............................................ 42

Chapter 6. Installing the Base component for Windows .................................. 47
Planning for the installation ................................................... 47
Base component installation CD ............................................ 47
Base component installation archive ....................................... 47
Supported languages and locales ............................................ 47
Preparing the system for the installation of the Base component for Windows ......................................................... 47
Installation prerequisites ....................................................... 47
Installing the Subsystem for UNIX-based Applications (required) ......................................................... 48
Installing the Utilities and SDK Package (required) ................. 48
Verifying the directory structure (required) ............................... 48
Ensuring that the Administrator UID is set to the correct value ........................................................................ 49
Checking the administrator UID ............................................. 49
Specifying the administrator UID and GID ............................... 49
Verifying and updating TCP/IP configuration files (required) ...... 49
Updating the DNS or hosts file (required) ............................... 50
Configuring the Subsystem for UNIX-based Applications ........... 50
Enabling the syslog daemon .................................................. 51
Enabling telnet login to Subsystem for UNIX-based Applications (Optional) ......................................................... 52
Installing the Base component for Windows ............................ 52
Verifying the installation ....................................................... 59
Chapter 1. Installing the Base component for AIX and Linux

This chapter describes how you install, configure, migrate, uninstall, and service the Base component of IBM Tivoli System Automation for AIX and Linux:

- “Planning for the installation.”
- “Preparing for installation” on page 6
- “Installing and upgrading the Base component” on page 9
- “Uninstalling the Base component for AIX and Linux” on page 41
- “Installing service” on page 67

Planning for the installation

Coexistence with other products

The Base component for AIX and Linux can coexist with the following IBM products:
- Cluster Systems Management (CSM)
- General Parallel File System (GPFS), V2R2 or higher

If these products are installed, they share packages with the Base component.

To check if CSM, GPFS, or both are installed, use the following commands:

On Linux systems:
- To check for GPFS, enter:
  `rpm -q gpfs`
- To check for CSM, enter:
  `rpm -q csm`

On AIX systems:
- To check if GPFS is installed, enter:
  `lslpp -l gpfs`
- To check if CSM is installed, enter:
  `root@node06 "# lslpp -l csm"`

Contents of the CD

The CD labeled “IBM Tivoli System Automation for Multiplatforms 2.3 Base component all Platforms” contains scripts and software packages for each platform and the corresponding architecture.

CDs / archives for the Base component

When you order the Base component of IBM Tivoli System Automation, you find it on the following CD/in the following archive:

Base component CD
To install the Base component, you use the installation script listed in the right column of the table below.
Table 1. Product CD versions

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Product CD label</th>
<th>Installation script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux &amp; AIX</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 Base component all platforms</td>
<td>SAM2300Base/installSAM</td>
</tr>
</tbody>
</table>

Electronic distribution of IBM Tivoli System Automation

If you prefer electronic distribution to delivery on the CD, we offer you the possibility to download the product from the Web. After you have purchased IBM Tivoli System Automation, you get an URL where you can download a tar file for the Linux and AIX operating systems.

Archives

Linux:

Table 2. Archives for Linux platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C100PML.tar</td>
<td>This is the archive you use to install the product. For extracting the archive, GNU tar 1.13 or later is required. Use the tar xf command to extract the archive. When you have extracted the files, you find the installation script installSAM in the following directory: SAM2300Base</td>
</tr>
</tbody>
</table>

AIX:

Table 3. Archives for AIX platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C100MML.tar</td>
<td>This is the archive you use to install the product. Use the tar xf command to extract the archive. When you have extracted the files, you find the installation script installSAM in the following directory: SAM2300Base</td>
</tr>
</tbody>
</table>

Supported platforms

The Base component for AIX and Linux of IBM Tivoli System Automation, Version 2.3, supports Linux on System z, System x, System i, and System p, and AIX 5.2 and AIX 5.3.

The Base component for AIX and Linux runs on all IBM eServer machines running Linux, and on IBM eServer System p machines running AIX.

The following table lists the supported Linux distributions and AIX versions. For the latest information, refer to the IBM Tivoli System Automation for Multiplatforms Release Notes on the IBM Tivoli System Automation for Multiplatforms home page:

The latest version of the release notes are available behind the Technical Documentation link.

Table 4. Supported platforms for the Base component of IBM Tivoli System Automation for Multiplatforms

<table>
<thead>
<tr>
<th></th>
<th>System x</th>
<th>System z</th>
<th>System p</th>
<th>System i</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUSE SLES 9 (32 bit)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 9 (64 bit)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 10 (32 bit)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 10 (64 bit)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RedHat RHEL 4.5 (32 bit)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RedHat RHEL 4.5 (64 bit)</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RedHat RHEL 5.0 (32 bit)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RedHat RHEL 5.0 (64 bit)</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>AIX 5.2</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>AIX 5.3</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes:
1. xSeries (except Intel IA64 based servers) and any other 32-bit Intel based server, or AMD Opteron based server (64-bit), or Intel EM64T based server (64 bit).
2. Requires SUSE SLES9 SP1
3. Requires C++ Runtime Library for AIX version 7.0.0.1, which is included in PTFs U800738 and U800739.
   For DB V9R1, which is shipped with IBM Tivoli System Automation for Multiplatforms V2R3, AIX version 8.0.0.4 is required.
4. SP1 must be installed.

Supported network interfaces
All platforms support 10 Megabit Ethernet, Fast Ethernet, and Gigabit Ethernet. In addition, the zSeries platform also supports Hipersockets, CTC, and VM Guest LAN.
Preparing for installation

The Base component of IBM Tivoli System Automation is contained in several packages that must be installed on every cluster node that you want to automate. Package type and content depend on the operating system on which you are installing the Base component.

Notes:
1. The software packages must be available on the nodes on which you want to install the Base component. For example, you can mount the CD-ROM on a PC and use FTP to transfer the files to the node, or you can install the packages over a shared Network File System.
2. To be sure that the software packages are installed and uninstalled in the correct order, use the Base component scripts **installSAM** and **uninstallSAM**.

### Table 5. Software packages available for installation, based on your operating system

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Type of package</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>RPM packages</td>
<td>IBM Tivoli System Automation RPMs and RSCT RPMs. RSCT (Reliable Scalable Cluster Technology) is the infrastructure used by the Base component to provide clusters with improved system availability, scalability, and ease of use.</td>
</tr>
</tbody>
</table>
| AIX              | **installp** file sets | IBM Tivoli System Automation **installp** file sets only. The AIX implementation of RSCT is included as part of the AIX 5 operating system. However, a more recent level of RSCT may be required. The following RSCT APARs must be installed:  
  - IZ00913 (AIX 5.2)  
  - IZ00912 (AIX 5.3)  
  See the Tivoli System Automation Release Notes document to find out which RSCT APARs are required for Base component fix packs. The 32-bit version of Java 1.4 or Java 5 SR5 must be installed. |

**Prerequisites**

Before starting the installation you must fulfill these requirements:
- A Korn Shell must be installed.
- If you are using both the AIX 5.2 platform and the System Automation for Multiplatforms end-to-end automation adapter (see Chapter 18, “Configuring the...
end-to-end automation adapter of the Base component of IBM Tivoli System Automation for Multiplatforms, make sure to have a pam.conf file in the /etc directory. You can find a sample pam.conf file in the SAM2300Base/AIX directory.

- Perl is required to use the command line interface of IBM Tivoli System Automation for Multiplatforms including native RSCT commands. It is by default installed on your Linux or AIX systems as part of the operating system, but if you are using IBM Tivoli System Automation in a language other than English, a special version of Perl may be required. Due to known problems with Perl 5.8.0 and how it handles UTF-8 encoded locales, some characters may not be properly displayed. This can occur on systems with Perl 5.8.0 installed, while using a UTF-8 encoded locale. When previous or subsequent versions of Perl are used, or non-UTF-8 encoded locales are used, this problem does not occur. AIX 5.2 uses Perl 5.8.0 and there is currently no opportunity to order a different version of Perl for that AIX release.

If you decide to upgrade your Perl 5.8.0 version on a Linux distribution, perform the following steps:

2. Unzip and tar -xvf on any directory.
3. Compile and install on the UTF-8 machine, referring the instruction provided with the downloaded files.
4. Change the symbolic link pointing to the directory of the Perl version that is used by IBM Tivoli System Automation from: /usr/sbin/rsct/perl5/bin/perl -> /usr/bin/perl to the directory where the new version of Perl is per default installed:
   /usr/sbin/rsct/perl5/bin/perl -> /usr/local/bin/perl.

- Also make sure that the directories /usr/sbin and /opt have at least 100 MB free space, and that the directory /var also provides at least 100 MB free space.
- On any node where the adapter can run at least 128 MB RAM must be available.
- During installation of IBM Tivoli System Automation on AIX the correct level of RSCT will be checked and a higher level of RSCT may be required. If this is required for your systems, download and install the appropriate RSCT filesets from the AIX service center.
- For other operating system-specific requirements, see the requirements Web page at http://www-306.ibm.com/software/tivoli/products/sys-auto-linux/requirements.html
- For languages using the double-byte character set (DBCS), the Telnet dialog buffer must be sufficiently large to ensure that long messages are properly displayed. If this is not the case, enlarge the Telnet dialog buffer.
- In the current RedHat 5 distributions, the SELinux environment is switched on by default. It must be switched off for IBM Tivoli System Automation to work properly.

**Initial configurations**

You must perform these initial configurations:

- On all nodes, set the environment variable CT_MANAGEMENT_SCOPE to 2 (peer domain scope) for all users of IBM Tivoli System Automation:
  
  **CT_MANAGEMENT_SCOPE=2**

  To permanently set the variable, set it in the profile.
- Make sure that the environment variable LANG is set to one of the supported locales for the root user. To set the environment variable, use the command:
export LANG=xx_XX

where xx_XX denotes one of the supported languages.
Installing and upgrading the Base component

This section covers the following topics:

- If you are performing an initial installation of the Base component, see the topic “Installing the Base component for AIX and Linux” below.
- If a previous version of the Base component is already installed, you need to perform some steps before the new version of the Base component can be installed. To perform a migration to a new version of the product, see the topic “Migrating the Base component” on page 12.

Installing the Base component for AIX and Linux

You use an installation script to install the Base component. The installation script performs the following actions:

- A complete prerequisites check to verify that all prerequisites are available and at the required level. If your system does not pass the check, the installation does not start, and you need to provide the missing prerequisites and restart the installation.
- Installs the Base component, including the end-to-end automation adapter.

To avoid having to restart the installation, you can invoke the prerequisites check separately, before starting the installation.

Performing the prerequisites check

Complete the following steps:

1. If you downloaded the tar file from the Internet, extract the file, using the following command:
   
   ```bash
   tar -xvf <tar file>
   ```
   
   If you got the product on a CD, mount the CD and change to the directory where the CD is mounted.

2. Enter:
   
   ```bash
   cd SAM2300Base
   ```

3. To start the prerequisites check, issue the following command:
   
   ```bash
   ./prereqSAM
   ```

   Typically, you do not need to specify any of the options that are available for the `prereqSAM` command. For a detailed description of the command, refer to the [IBM Tivoli System Automation for Multiplatforms Base Component Reference](https://www.ibm.com/support/knowledgecenter/STWQHT_w11_pci0/).

4. When the check is complete, check the following log file for information about missing prerequisites:
   
   ```bash
   /tmp/prereqSAM.<#>.log
   ```

   where <#> is a number; the highest number identifies the most recent log file.

5. If your system did not pass the prerequisites check, correct any problems before starting the installation.

Installing the Base component

Before you begin:

If an RSCT peer domain already exists, ensure that the node on which you are invoking the script is offline in the domain. Otherwise, the installation will be canceled.
To install the product, including the automation adapter, perform the following steps:

1. If you downloaded the tar file from the Internet and have not yet extracted the file, extract it using the following command:
   ```
   tar -xvf <tar file>
   ```
   If you got the product on a CD, mount the CD and change to the directory where the CD is mounted.

2. Enter:
   ```
   cd SAM2300Base
   ```

3. Invoke the installation script:
   ```
   ./installSAM
   ```
   Typically, you do not need to specify any of the options that are available for the `installSAM` command. For a detailed description of the command, refer to the [IBM Tivoli System Automation for Multiplatforms Base Component Reference](#).

4. Read the information in the License Agreement and the License Information that is displayed. You can scroll forward line by line using the “Enter” key, and page by page using the “spacebar”, which is basically the “more” functionality in UNIX®. Once you have scrolled to the bottom of the License information file and you want to accept the terms of the license agreement, type ‘y’. Any other input will cancel the installation.
   The installation is also canceled when no license file is found.

5. After you accept the license agreement, the installation program performs a complete prerequisites check to verify that all prerequisites are available and at the required level.
   If your system does not pass the check, the installation does not start, and you need to provide the missing prerequisites and restart the installation.
   Information about the results of the prerequisites check is available in the log file `/tmp/installSAM.<#>.log` (for details, see step [4]).
   If your system passed the check, the product, including the automation adapter, is installed.

6. Check the following log file for information about the installation:
   `/tmp/installSAM.<#>.log`
   where `<#>` is a number; the highest number identifies the most recent log file.
   The entries in the log file have the following prefixes:
   ```
   prereqSAM
   ```
   Entries that were written during the prerequisites check.
   ```
   installSAM
   ```
   Entries that were written during the installation of the product.

7. To find out which packages were installed, issue the following command:
   ```
   • AIX:
     lslpp -l sam*
   • Linux:
     rpm -qa | grep -E "^src|^rsct|^sam$"
   ```
   See the rpm man page for details about the rpm command.

Post-installation task
When you have installed the Base component, perform the following tasks:
Configure the system logger on AIX
The system logger is not configured by default. Messages are written to the error log.
To be able to obtain the debug data, it is recommended that you configure the system logger in the file /etc/syslog.conf. When you have made the necessary changes, you must recycle the syslogd using the command
\texttt{refresh -s syslogd}. The location of the log file is defined in /etc/syslog.conf.

Installing the product license
IBM Tivoli System Automation requires that a valid product license is installed on each system it is running on. The license is contained on the installation medium in the 'license' sub directory. The installation of the license is usually performed during the product installation process. In case this did not succeed, issue the following command to install the license:
\texttt{samlicm -i license_file}

In order to display the license, issue:
\texttt{samlicm -s}

See the \textit{IBM Tivoli System Automation for Multiplatforms Base Component Reference} for a detailed description of the \texttt{samlicm} command.

Upgrading from a Try & Buy license to a full product license
If you have installed the Try & Buy version of the IBM Tivoli System Automation for Multiplatforms Base component and then purchase the full product version, you will receive another copy of the installation media, which contains the license file for the full license.

The license file is located on the installation medium in the license subdirectory. It is recommended to perform the license upgrade by issuing the following command:
\texttt{samlicm -i <license_file_name>}

In order to display the license, issue:
\texttt{samlicm -s}

(See “Installing the product license.”)

After upgrading the license, you should check if any updates for IBM Tivoli System Automation for Multiplatforms are already available and install the latest service level.

Languages and locales supported by the Base component
If you want to use the Base component in a language other than English, or if your default system locale is a non-English locale, use the following sections to find out which languages and locales are supported.

Turkish locales are not supported by the Base component on any platform.

Base component for Linux
Table 6 on page 12 shows the combinations of languages and locales that are supported for the Base component on Linux systems to display translated
messages. New versions of Linux operating systems may not support all of the listed encodings. UTF-8 encoding is always supported.

Table 6. Languages and locales supported by the Base component on Linux systems

<table>
<thead>
<tr>
<th>Language</th>
<th>UTF-8</th>
<th>ISO-8859-1</th>
<th>EUC/GBK</th>
<th>Euro</th>
<th>GB18030/BIG5</th>
</tr>
</thead>
<tbody>
<tr>
<td>German</td>
<td>de_DE.UTF-8</td>
<td>de_DE, de_DE.ISO-8859-1</td>
<td></td>
<td>de_DE@euro</td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>es_ES.UTF-8</td>
<td>es_ES, es_ES.ISO-8859-1</td>
<td></td>
<td>es_ES@euro</td>
<td></td>
</tr>
<tr>
<td>French</td>
<td>fr_FR.UTF-8</td>
<td>fr_FR, fr_FR.ISO-8859-1</td>
<td></td>
<td>fr_FR@euro</td>
<td></td>
</tr>
<tr>
<td>Italian</td>
<td>it_IT.UTF-8</td>
<td>it_IT, it_IT.ISO-8859-1</td>
<td></td>
<td>it_IT@euro</td>
<td></td>
</tr>
<tr>
<td>Japanese</td>
<td>ja_JP.UTF-8</td>
<td>ja_JP.eucJP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Korean</td>
<td>ko_KR.UTF-8</td>
<td>ko_KR.eucKR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazilian Portuguese</td>
<td>pt_BR.UTF-8</td>
<td>pt_BR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>zh_CN.UTF-8</td>
<td>zh_CN.GBK, zh_CN.GB2312</td>
<td></td>
<td>zh_CN.GB18030</td>
<td></td>
</tr>
<tr>
<td>Traditional Chinese</td>
<td>zh_TW.UTF-8</td>
<td>zh_TW</td>
<td></td>
<td></td>
<td>zh_TW.BIG5, zh_TW</td>
</tr>
</tbody>
</table>

### Base component for AIX

The table below shows the combinations of languages and locales that are supported for the Base component for AIX to display translated messages.

Table 7. Languages and locales supported by the Base component on AIX systems

<table>
<thead>
<tr>
<th>Language</th>
<th>UTF-8</th>
<th>ISO-8859-1</th>
<th>EUC/GBK</th>
<th>SJIS/GB18030/BIG5</th>
</tr>
</thead>
<tbody>
<tr>
<td>German</td>
<td>DE_DE</td>
<td>de_DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>ES_ES</td>
<td>es_ES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>French</td>
<td>FR_FR</td>
<td>fr_FR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italian</td>
<td>IT_IT</td>
<td>it_IT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Korean</td>
<td>KO_KR</td>
<td>ko_KR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazilian Portuguese</td>
<td>PT_BR</td>
<td>pt_BR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>ZH_CN</td>
<td>zh_CN</td>
<td></td>
<td>Zh_CN</td>
</tr>
<tr>
<td>Traditional Chinese</td>
<td>ZH_TW</td>
<td>zh_TW</td>
<td></td>
<td>Zh_TW</td>
</tr>
</tbody>
</table>

### Migrating the Base component

You can migrate to IBM Tivoli System Automation V2R3 if IBM Tivoli System Automation V2R2 is already installed.

Review the following considerations before migrating one or more nodes to a newer level:

- The migration process starts when any node within the active cluster is upgraded to the higher code level.
- You can always upgrade to a higher code level. Downward migration is not possible.
• The migration process is only complete when the active version number is equal to the highest installed code version number. Until then, different code levels can coexist. See “Verifying the active and installed version number” on page 14 and “Completing the migration” on page 15 how to complete the migration process.

You can use one of the following procedures to migrate the IBM Tivoli System Automation Base component to a higher level:

• It is recommended to use the procedure described in “Migrating an entire domain” on page 9.
• “Performing a node-by-node migration”

**Migrating an entire domain**

During the migration, the domain will not be available. To minimize downtime, you can perform a prerequisites check before you start the actual migration (for more information, see “Performing the prerequisites check” on page 9).

To migrate an entire domain, perform these steps:

1. Make sure that all resources are offline:
   a. Check if the System Automation for Multiplatforms end-to-end automation adapter is running:
      ```bash
      samadapter status
      ```
      If it is running, stop the automation adapter:
      ```bash
      samadapter stop
      ```
   b. Stop all online resource groups by setting their NominalState to Offline:
      ```bash
      chrg -o Offline <resource-group-name>
      ```

2. If the domain is online, stop the domain:
   ```bash
   stoprpdomain <domain-name>
   ```

3. Run the `installSAM` script from the installation directory on all nodes. For more information on the `installSAM` script, see “Installing the Base component for AIX and Linux” on page 9.

4. Start the domain:
   ```bash
   startrpdomain <domain-name>
   ```

5. Check the code levels with the `Issrc -ls IBM.RecoveryRM` command (see the example in “Verifying the active and installed version number” on page 14). All nodes should have the newly installed code level, but the active code level should still be the previous one.

6. In order to activate the new version, continue with “Completing the migration” on page 15.

**Performing a node-by-node migration**

Migrating the nodes of a domain one by one has the advantage that IBM Tivoli System Automation remains available during the migration. To further minimize downtime, you can perform a prerequisites check before you start the actual migration (for more information, see “Performing the prerequisites check” on page 9).

To perform a node-by-node migration, do this:

1. Exclude the node from automation to ensure that resources that must be kept available are moved to another node in the peer domain:
   ```bash
   samctrl -u a <node>
   ```
Note that the move operations may take a moment.

2. Stop the node from another node in the domain, and verify that it is stopped:
   stoprpnode <node>; lsrpnode

3. To upgrade the node, run the script ./installSAM from the installation directory.
   For more information on the installSAM script, see “Installing the Base component for AIX and Linux” on page 9.

4. Start the node:
   startrpnode <node>

5. Include the upgraded node in automation again:
   samctrl -u d <node>

6. The upgraded node can now join the existing domain. Use the Issrc -ls IBM.RecoveryRM command (see the sample in “Verifying the active and installed version number”) to display the installed version and the active version of the product. The new code features will not be activated until the active IBM Tivoli System Automation version number is equal to the highest IBM Tivoli System Automation version number installed within the cluster, and you cannot fully utilize these new code features until all the nodes are upgraded.

7. Repeat the steps 1-6 for other nodes within the cluster.

8. In order to activate the new version continue with “Completing the migration” on page 15.

Verifying the active and installed version number

After the upgrade the new features of the new code are not yet activated. The previous and new code levels can coexist until the migration is complete. The Issrc -ls IBM.RecoveryRM command shows you the active version number AVN (2.1.0.0 in the sample below) and the installed version number IVN (2.2.0.0. in the sample below) of the product. When IVN and AVN are the same, migration is complete.

The output looks like:

Subsystem : IBM.RecoveryRM
PID : 27973
Cluster Name : ws
Node Number : 1
Daemon start time : Wed Nov 15 08:09:10 2006

Daemon State:
  My Node Name : lnxcm3x
  Master Node Name : lnxcm3x (node number = 1)
  Our IVN : 2.2.0.0
  Our AVN : 2.1.0.0
  Our CVN : 11082527751 {0x140861007}
  Total Node Count : 1
  Joined Member Count : 1
  Config Quorum Count : 1
  Startup Quorum Count : 1
  Operational Quorum State: HAS_QUORUM
  In Config Quorum : TRUE
  In Config State : TRUE
  Replace Config State : FALSE

Figure 1. Verifying the active and installed version numbers

In order to activate the new version, continue with “Completing the migration” on page 15.
Completing the migration

In order to check and complete the migration, perform the following steps:

1. Make sure that the domain is started and that all nodes in the domain are online.

2. Issue the `lsrpdomain` command to display the version of RSCT that is active in the peer domain, and the mixed version status:

<table>
<thead>
<tr>
<th>Name</th>
<th>OpState</th>
<th>RSCTActiveVersion</th>
<th>MixedVersions</th>
<th>TSPort</th>
<th>GSPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA_Domain</td>
<td>Online</td>
<td>2.4.4.1</td>
<td>Yes</td>
<td>12347</td>
<td>12348</td>
</tr>
</tbody>
</table>

3. Issue the `lsrpnode` command to display which version of RSCT that is installed on the nodes. Keep in mind that all nodes must be online:

<table>
<thead>
<tr>
<th>Name</th>
<th>OpState</th>
<th>RSCTVersion</th>
</tr>
</thead>
<tbody>
<tr>
<td>node01</td>
<td>Online</td>
<td>2.4.5.4</td>
</tr>
<tr>
<td>node02</td>
<td>Online</td>
<td>2.4.5.4</td>
</tr>
<tr>
<td>node03</td>
<td>Online</td>
<td>2.4.5.4</td>
</tr>
</tbody>
</table>

4. If the RSCT peer domain is running in mixed version mode (MixedVersions = Yes) and all nodes have been upgraded to the new release of IBM Tivoli System Automation, you must update the active RSCT version by running the RSCT CompleteMigration action on one of the nodes. Before running the action, review the RSCT migration preparation procedures in the *IBM RSCT Administration Guide*.

   To update the RSCTActiveVersion, make sure that all nodes are online, and issue the following command on one of the nodes:

   ```
   runact -c IBM.PeerDomain CompleteMigration Options=0
   ```

   To verify that the active RSCT version has been updated, issue the `lsrpdomain` command again:

<table>
<thead>
<tr>
<th>Name</th>
<th>OpState</th>
<th>RSCTActiveVersion</th>
<th>MixedVersions</th>
<th>TSPort</th>
<th>GSPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA_Domain</td>
<td>Online</td>
<td>2.4.5.4</td>
<td>No</td>
<td>12347</td>
<td>12348</td>
</tr>
</tbody>
</table>

5. Run the `samctrl -m` command to activate the new features of the new code and to finish the migration. For more information about the command, refer to the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*.

The code version of the ActiveVersion and the InstalledVersion of IBM Tivoli System Automation should now be the same for all nodes. Until this is true, the new code features have not been activated and cannot be used.
Chapter 2. Installing the Base component operations console

Planning for the installation

Packaging
When you order the Base component of IBM Tivoli System Automation, you find the operations console on the following CD and in the following archive, respectively:

Operations console CD
The following table lists the versions of the operations console CDs that are available for the Base component. To install the operations console, you use the installation wizard file listed in the right column of the table.

Table 8. Product CD versions

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Product CD label</th>
<th>Installation wizard file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows*</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 Base component, Operations Console for Windows</td>
<td>EEZ2300E2EWindows\Windows\setup.exe</td>
</tr>
<tr>
<td>AIX</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 Base component, Operations Console for AIX</td>
<td>EEZ2300E2EAIX/AIX/setup.bin</td>
</tr>
<tr>
<td>Linux on System x</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 Base component, Operations Console for Linux on System x</td>
<td>EEZ2300E2E1386/i386/setup.bin</td>
</tr>
<tr>
<td>Linux on POWER</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 Base component, Operations Console for Linux on POWER</td>
<td>EEZ2300E2EPPC/pc/setup.bin</td>
</tr>
<tr>
<td>Linux on System z</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 Base component, Operations Console for Linux on System z</td>
<td>EEZ2300E2ES390/s390/setup.bin</td>
</tr>
</tbody>
</table>

* The Base component operations console can be installed on Windows systems and used to access and work with first-level automation domains for which an automation adapter is available (for example, the Base component for AIX and Linux and HACMP). It cannot be used to access the IBM Tivoli System Automation for Multiplatforms Base component on Windows.

Electronic distribution
You can also obtain the Base component through electronic distribution. In this case, you can download the deliverables from a URL you receive after purchasing the product.

For each platform, one archive is available for installing the operations console. The archives are listed in the following tables.
**Windows:**

*Table 9. Archives for Windows platforms*

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C100HML.exe</td>
<td>This is the archive you use to install the operations console. The archive is self-extracting. When you have extracted the files, you find the installation wizard in the following directory: <code>&lt;drive&gt;:\EEZ2300E2E\Windows\Windows\setup.exe</code> For example: <code>C:\EEZ2300E2E\Windows\Windows\setup.exe</code></td>
</tr>
</tbody>
</table>

**AIX:**

*Table 10. Archives for AIX platforms*

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C100JML.bin</td>
<td>This is the archive you use to install the operations console. The archive is self-extracting. When you have extracted the files, you find the installation wizard in the following directory: <code>EEZ2300E2E\AIX\setup.bin</code></td>
</tr>
</tbody>
</table>

**Linux on System x:**

*Table 11. Archives for Linux on System x*

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C100JML.tar</td>
<td>This is the archive you use to install the product. Use the <code>tar -xf</code> command to extract the archive. When you have extracted the files, you find the installation wizard in the following directory: <code>EEZ2300E2E\i386\setup.bin</code></td>
</tr>
</tbody>
</table>

**Linux on POWER:**

*Table 12. Archives for Linux on POWER*

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C100KML.tar</td>
<td>This is the archive you use to install the product. Use the <code>tar -xf</code> command to extract the archive. When you have extracted the files, you find the installation wizard in the following directory: <code>EEZ2300E2E\ppc\setup.bin</code></td>
</tr>
</tbody>
</table>
Linux on System z:

Table 13. Archives for Linux on System z

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C100LML.tar</td>
<td>This is the archive you use to install the product. Use the <code>tar -xf</code> command to extract the archive. When you have extracted the files, you find the installation wizard in the following directory: EEZ2300E2ES390/s390/setup.bin</td>
</tr>
</tbody>
</table>

Product requirements

The following sections list the software and hardware requirements for the operations console. For the latest information, refer to the IBM Tivoli System Automation for Multiplatforms Release Notes. To obtain a copy of the release notes, go to the IBM Tivoli System Automation for Multiplatforms home page and click Technical Documentation. The IBM Tivoli System Automation home page is located at:


Supported platforms

The following table lists the platforms that are supported for the Base component operations console:

Table 14. Supported operating systems

<table>
<thead>
<tr>
<th>Operating system</th>
<th>System x³</th>
<th>System i</th>
<th>System p</th>
<th>System z</th>
</tr>
</thead>
<tbody>
<tr>
<td>(32 bit)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(32 bit)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIX 5.2</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(AIX 5L Version 5.2) ML 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIX 5.3</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>(AIX 5L Version 5.3) ML 2⁴</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 9 (32 bit³)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 9 (64 bit³)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SUSE SLES 10 (32 bit³)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 10 (64 bit³)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Table 14. Supported operating systems (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>System x</th>
<th>System i</th>
<th>System p</th>
<th>System z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat RHEL 4.0 AS (32 bit)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat RHEL 4.0 AS (64 bit)</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Red Hat RHEL 5.0 AS (32 bit)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat RHEL 5.0 AS (64 bit)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Notes:
1. IBM x/Series systems with IA32, EM64T, or AMD64 architecture.
   Any other systems with IA32, EM64T, or AMD64 architecture are also supported.
   Systems with IA64 architecture are not supported.
2. The following Linux kernel architectures are supported for running with 32 bit:
   • x86 on IBM System x
3. The following Linux kernel architectures are supported for running with 64 bit:
   • ppc64 on IBM System i and IBM System p
   • s390x on IBM System z is supported for some distributions
4. APAR IY65979 must be installed

Supported Web browsers
The operations console is displayed in a Web browser. The browser connects to the embedded version of IBM WebSphere Application Server in which the operations console is running. The Web browser may run on an arbitrary system.

The following Web browsers are supported:
• Microsoft Internet Explorer V6.0 SP1
• Mozilla V1.7.8
• Firefox V1.5

For information on how the Web browser must be configured, refer to the IBM Tivoli System Automation for Multiplatforms Base Component Administrator’s and User’s Guide section "Configuring your Web browser".

Hardware requirements

System Memory: 1.0 GB is required on the server on which the operations console is to be installed.

Disk space requirements: The following table lists the disk space requirements on Windows systems.
### Table 15. Disk space requirements for the installation on Windows systems

<table>
<thead>
<tr>
<th>Description</th>
<th>Default directory</th>
<th>Disk space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base component operations console installation directory (including the embedded version of WebSphere Application Server)</td>
<td>C:\Program Files\IBM\tsamp\eez</td>
<td>400 MB</td>
</tr>
<tr>
<td>Temporary disk space required for the installation and for installation log and response files</td>
<td>The value of the system variable %TEMP%. Typically this is: \C:\Documents and Settings\Administrator\Local Settings\Temp</td>
<td>125 MB</td>
</tr>
<tr>
<td>Tivoli Common Directory</td>
<td>C:\Program Files\IBM\tivoli\common\eez</td>
<td>250 MB</td>
</tr>
<tr>
<td>Installer registry</td>
<td>The Zero G Registry resides in the hidden directory</td>
<td>10 KB</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Zero G Registry\com.zerog.registry.xml</td>
<td></td>
</tr>
</tbody>
</table>

The following table lists the disk space requirements on AIX and Linux systems:

### Table 16. Disk space requirements on AIX and Linux systems

<table>
<thead>
<tr>
<th>Description</th>
<th>Default directory</th>
<th>Disk space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base component operations console installation directory (including the embedded version of WebSphere Application Server)</td>
<td>/opt/IBM/tsamp/eez</td>
<td>420 MB</td>
</tr>
<tr>
<td>Temporary disk space required for the installation</td>
<td>/tmp</td>
<td>300 MB</td>
</tr>
<tr>
<td>Tivoli Common Directory</td>
<td>/var/ibm/tivoli/common/eez</td>
<td>250 MB</td>
</tr>
<tr>
<td>Installer registry</td>
<td>/var/.com.zerog.registry.xml</td>
<td>10 KB</td>
</tr>
</tbody>
</table>

### Preparing for the installation of the Base component operations console

#### Collecting the information you need to provide during installation

The installation of the operations console is wizard-driven. The wizard guides you through the installation and prompts you for installation and configuration parameters. The following tables list the parameters you need to specify on the installation wizard panels in the order in which they must be specified.

Make sure that you specify all required parameters on the installation wizard panels and that your entries are correct. The installation wizard does not verify that you entries are correct and complete during the installation.

### Installation directory and Tivoli Common Directory

The parameters listed in the following table must always be specified.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation directory name</td>
<td>The directory to which the installable features are installed. In this guide, this directory is referred to as EEZ_INSTALL_ROOT. When specifying a directory other than the default, observe the following restrictions: Windows: • The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9). • The colon character is allowed only once, immediately following the drive letter. For example, C:&lt;directory_name&gt; is allowed, but C:&lt;directory_name&gt;:&lt;directory_name&gt; is not allowed. • The space character and the underscore character (<em>) are allowed. AIX, Linux: • The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9). • The underscore character (</em>) is allowed. • The space and colon characters are not allowed.</td>
<td>Windows: C:\Program Files\IBM\tsamp\eez AIX, Linux: /opt/IBM/tsamp/eez</td>
</tr>
</tbody>
</table>
Table 17. Installation directory and Tivoli Common Directory (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Common Directory</td>
<td>The Tivoli directory for storing serviceability information.</td>
<td>Windows:</td>
</tr>
<tr>
<td></td>
<td>During installation, you are only prompted for input when no Tivoli Common Directory is found on the system.</td>
<td>C:\Program Files\IBM\tivoli\common</td>
</tr>
<tr>
<td></td>
<td>In the Tivoli Common Directory, the subdirectory eez is created for storing product-specific data.</td>
<td>AIX, Linux:</td>
</tr>
<tr>
<td></td>
<td>When specifying a directory other than the default, observe the following restrictions:</td>
<td>/var.ibm/tivoli/common</td>
</tr>
<tr>
<td></td>
<td><strong>Windows:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The colon character is allowed only once, immediately following the drive letter. For example, C:&lt;directory_name&gt; is allowed, but C:&lt;directory_name&gt;:&lt;directory_name&gt; is not allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The space character and the underscore character (_) are allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AIX, Linux:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The underscore character (_) is allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The space and colon characters are not allowed.</td>
<td></td>
</tr>
</tbody>
</table>

**Installation parameters for the Base component operations console**

The parameters listed in the following table must always be specified.
## Table 18. Installation parameters for Integrated Solutions Console

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
</table>
| **WAS Admin User ID**                          | The ID of the administrator user for the embedded version of WebSphere Application Server, which the Base component operations console uses as run-time environment. The user ID only has administrative privileges for the WebSphere Application Server but is not authorized to perform any Tivoli System Automation tasks.  
  The user ID must comply with the following conditions:  
  • The user ID must be unique.  
  • The length is 3 to 60 characters.  
  • A valid user ID may contain only the characters a-z, A-Z, period (.), hyphen (-), underscore (_), and double-byte character set (DBCS) characters.  
  No other characters are permitted in this field. For example, diacritics, such as the umlaut, are not permitted. | No default value is provided |**Password**                    | The password for the WAS Admin User ID.  
  The password must comply with the following conditions:  
  • The length is 5 to 60 characters.  
  • A valid password may contain only the characters a-z, A-Z, period (.), hyphen (-), and underscore (_).  
  No other characters are permitted in this field. For example, DBCS characters and diacritics, such as the umlaut, are not permitted. | No default value is provided |**Tivoli System Automation Administration User ID** | The user ID of the administrator user for Tivoli System Automation. The user is authorized to perform Tivoli System Automation tasks, but cannot perform WebSphere Application Server tasks.  
  Notes:  
  1. The user can only be logged in from a single location (for example, a browser window).  
  2. If multiple users are to work with the operation console concurrently, personalized user IDs must be created and assigned to the predefined user groups. To create these user IDs, this Tivoli System Automation administrator user ID must be used. | eezadmin                |

### Port assignment for the embedded version of IBM WebSphere Application Server

The following table lists the default ports for the embedded version of IBM WebSphere Application Server.

**Notes:**

1. If a WebSphere Application Server is already installed on the system or if a previous installation was not removed complete and cleanly, the ports are incremented by the installation program without notice.

2. You can check the ports of an embedded WebSphere Application Server installation in the following file:  
   `<was_home>/profiles/<profileName>/properties/portdef.props`  
   The default `<was_home>` directory is:  
   On AIX and Linux systems:  
   `/opt/IBM/tsamp/eez/ewas/AppServer`  
   On Windows systems
3. WebSphere Application Server will fail to start if the ports are used by another application at start time.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>WC Default Host</td>
<td>The number of the HTTP port for the embedded version of IBM WebSphere Application Server. This value must not conflict with existing port assignments on the system.</td>
<td>9080</td>
</tr>
<tr>
<td>WC Default Host Secure</td>
<td>The port that the embedded version of IBM WebSphere Application Server will use for secure HTTP transport (HTTPS). This value must not conflict with existing port assignments on the system.</td>
<td>9443</td>
</tr>
<tr>
<td>WC Admin Host</td>
<td>The HTTP Administrative Console port on the embedded version of IBM WebSphere Application Server. This value must not conflict with existing port assignments on the system.</td>
<td>9060</td>
</tr>
<tr>
<td>WC Admin Host Secure</td>
<td>The HTTPS Administrative Console secure port on the embedded version of IBM WebSphere Application Server. This value must not conflict with existing port assignments on the system.</td>
<td>9043</td>
</tr>
<tr>
<td>Domain RMI Auth Port</td>
<td>The address for the bootstrap function and the port number for the Java Remote Method Invocation (RMI) connector on the embedded version of IBM WebSphere Application Server. This value must not conflict with existing port assignments on the system.</td>
<td>2809</td>
</tr>
<tr>
<td>SOAP Connector Address</td>
<td>The address for the Simple Object Access Protocol (SOAP) connector on the embedded version of IBM WebSphere Application Server. This value must not conflict with existing port assignments on the system.</td>
<td>8880</td>
</tr>
</tbody>
</table>

### Installation prerequisites

The following prerequisites must be satisfied before you can start the installation wizard for the operations console:

- The user ID that is used to run the installation program must have administrator authority.
  - On Linux and AIX, this user ID is typically "root".
- When installing the operations console to an AIX or Linux system, be sure that an XWindows session is available for displaying the graphical installation program.
- In current RedHat 5 distributions, the SElinux environment is switched on by default. It must be switched off for IBM Tivoli System Automation to work properly.
Installing the Base component operations console using the graphical installation program

To install the Base component operations console, you have two options:

- You can use a graphical installation program, the so-called installation wizard.
- You can install the operations console in silent mode, using a response file you generated in a previous wizard-driven installation.

This section describes how to install the Base component operations console using the installation wizard. The required steps are described below.

Make sure that you specify all required parameters on the installation wizard panels and that your entries are correct. The installation wizard does not verify that you entries are correct and complete during the installation.

The screens in this section show a Linux installation. The screens that are displayed for other operating systems have a similar appearance. Make sure to conform to the conventions of your platform when specifying directory locations, files names, and so on.

To install the Base component operations console, perform these steps:

1. Insert the following CD into the CD drive:
   
   IBM Tivoli System Automation Multiplatforms V2.3.0 Base component, Operations Console for `<operating_system_name>`

   There are multiple CDs. Be sure to use the one for your platform.

2. Change to the directory that contains the installation program using the `cd` command. For the location of the directory, refer to "Packaging" on page 17.

3. Launch the installation wizard by starting the following program from the current working directory:
   
   **Windows**: `setup.exe`
   
   To generate a response file for use in a silent installation, use the following command to launch the wizard:
   
   `setup.exe -Dpreparesilent=true`
   
   **AIX, Linux**: `setup.bin`
   
   To generate a response file for use in a silent installation, use the following command to launch the wizard:
   
   `setup.bin -Dpreparesilent=true`

   When the installation wizard is ready, the initial wizard window appears:
4. Select the language in which the text on the installation wizard window is to appear and click OK. The language in which the Base component is installed is derived from the system’s locale setting.

5. Read the information on the Introduction window and click Next.
6. Carefully read the terms of the license agreement. Make sure to also read the non-IBM terms by clicking Read non-IBM terms.

To accept the terms of the license agreement, select I accept both the IBM and the non-IBM terms and click Next.

7. Specify the installation directory or accept the default location.
   Click Next.

8. If the installation program detected a Tivoli Common Directory on your system, for example, because a Tivoli product is already installed, the directory must also be used for IBM Tivoli System Automation for Multiplatforms. In this case, the entry field that is displayed in this window is write-protected.
If the installation program did not detect a Tivoli Common Directory on your system, accept the default location or specify the directory to which the Tivoli log files are to be written.

Click Next.

9. Specify the user ID and password of the WebSphere administrator user. Click Next.

10. If no other WebSphere Application Server is installed on the system, accept the default ports for the embedded version of IBM WebSphere Application Server. To change any of the values, select Change default ports and make your changes.
**Note:** If you leave the values unchanged and another WebSphere Application Server is detected on the system, the ports will be changed without notice.

Click Next.

12. Review the information in the summary window and ensure that sufficient disk space is available.
Click **Install** to start the installation.

**Note:** To clean up the system from a partial installation, use the uninstallation program.

13. During the installation phase, information windows like the following inform you of the progress.

14. The following window is displayed during the configuration phase:
Note: You may cancel the installation at any time. If you cancel during the configuration phase, the installer performs no cleanup. You can re-invoke the installation again later and configuration will resume at the point where it was canceled, or you can run the uninstallation program to clean up the system.

15. Review the information in the Installation Complete window. It informs you whether the installation completed successfully or whether errors occurred or the installation was canceled during the configuration process. Click Done to close the installation wizard.
Installing the Base component operations console in silent mode

You can install the Base component operations console in silent mode, using a response file you generated in a wizard-driven installation (see “Installing the Base component operations console using the graphical installation program” on page 26).

After the wizard-driven installation is complete, you find the response file install.properties in the following directory:

<EEZ_INSTALL_ROOT>/install

Note that this files is always generated even if you did not specify the option -Dpreparesilent=true when you invoked the installation wizard. However, install.properties files created without the -Dpreparesilent=true option cannot be used for silent installation.

To install the operations console in silent mode, perform these steps:

1. Copy the response file install.properties file to the system on which you want to perform the installation.
2. To start the installation, issue this command:
   AIX, Linux:
   ```
   setup.bin -i silent -f <fully_qualified_properties_file_name>
   ```
   Windows:
   ```
   setup.exe -i silent -f <fully_qualified_properties_file_name>
   ```

Verifying the installation

Perform the following steps to verify that the Base component operations console was installed successfully:

1. In a Web browser window, specify the following address to display the Login panel of Integrated Solutions Console:
   ```
   http://<your_host_name>:<your_isc_port>/ibm/console
   ```

   The default port is 9060.
2. Enter the WebSphere administrator user ID and the corresponding password. If the Welcome page of Integrated Solutions Console is displayed, the embedded version of WebSphere Application Server was installed successfully. Log off.
3. Repeat step 1. On the Log in panel of Integrated Solutions Console, enter the System Automation administrator user ID. The default user ID is eeZadmin.

4. On the Welcome page of Integrated Solutions Console, click the entry for Tivoli System Automation for Multiplatforms. If the Welcome page of Tivoli System Automation for Multiplatforms is displayed, the Base component operations console was installed successfully.
Chapter 3. Upgrading the operations console from release 2.2

An upgrade from release 2.2 to release 2.3 is not possible. To obtain release 2.3, uninstall release 2.2 and install release 2.3.
Chapter 4. Configuring the operations console

Configuring the end-to-end automation adapter to use the operations console

The System Automation for Multiplatforms end-to-end automation adapter must be configured in order to be able to directly access the operations console. "Host using adapter tab" on page 165 describes how to do this.

See Chapter 18, “Configuring the end-to-end automation adapter of the Base component of IBM Tivoli System Automation for Multiplatforms,” on page 159 to learn more about the System Automation for Multiplatforms end-to-end automation adapter.

Configuring the operations console for direct access mode

This is necessary if your operations console cannot use port 2002 to receive events from adapters, or if you want to use the SSL (Secure Socket Layer) protocol for the transmission of requests from the operations console to the adapter.

Planning the configuration

If you want to change the port number, obtain a valid port number from your network administrator. Note that all adapters that are connected to the operations console must send events to the same "Event port".

The operations console supports the Secure Socket Layer (SSL) protocol but it does not enforce it on adapters. Whether SSL is used for transport must be specified for the adapter, for example, on the Security tab of the adapter configuration dialog (see “Security tab” on page 170). All adapters that require SSL must have the same truststore file, keystore file, alias name and password for the keystore specified. The operations console uses the same information. Therefore, the truststore file and the keystore file must be placed on the host of the operations console.

If no truststore and keystore keys have been generated yet, you can use ikeyman.bat to generate them. ikeyman.bat is available in the directory <isc_home>/AppServer/bin. The resulting information should be the location of truststore and keystore, and alias name and password to access the keystore. Note that actual keys would be obtained from a certification authority.

Using the configuration dialog

Perform the following steps to configure the operations console:

1. Invoke the configuration dialog:
   - Windows: Change the directory to C:\Program Files\IBM\tsamp\eez\bin and type cfgdirect.
   - AIX and Linux: Type cfgdirect. The configuration dialog is displayed. The fields on the dialog tab show the current settings.

2. The event port number on the Server tab specifies the port on which the operations console listens for events from the adapter.
3. In the fields on the Security tab you can specify the information required for using the SSL protocol (see “Planning the configuration” on page 39).

4. To save your changes, click Save.

5. Click Done to close the dialog.
Chapter 5. Uninstalling the Base component for AIX and Linux and the operations console

Uninstalling the Base component for AIX and Linux

Before you begin:

- Use the uninstallSAM script that is provided for your operating system to uninstall the Base component. For example, run ./uninstallSAM from the installation directory. This will ensure a proper deinstallation of the product.
- Before uninstalling you should save your configuration with the sampolicy –S command. For information on how to save IBM Tivoli System Automation, refer to the following documentation:
  - The description of the sampolicy command in the [IBM Tivoli System Automation for Multiplatforms Base Component Reference]
- uninstallSAM will remove all configuration information that you defined for the domain. Never use uninstallSAM before upgrading to a new version.

To uninstall IBM Tivoli System Automation perform the following steps:

1. Ensure that the domain is offline:
   - Check if a domain is still online by entering the command:
     ```bash
     lsrpdomain
     ```
   - In order to stop a domain enter the command:
     ```bash
     stoprpdomain <domain>
     ```

2. Uninstall the product with the uninstallSAM script:
   ```bash
   ./uninstallSAM
   ```
   Typically, you do not need to specify any of the options that are available for the uninstallSAM command. For a detailed description of the command, refer to the [IBM Tivoli System Automation for Multiplatforms Base Component Reference]
   If CSM or GPFS (which also use RSCT and System Resource Controller (SRC) packages) is installed on a Linux system from which you want to uninstall IBM Tivoli System Automation, RPM will ensure that RSCT and SRC will not be uninstalled with IBM Tivoli System Automation. RPM messages will indicate this.

3. Check the following log file for information about the uninstallation:
   ```bash
   /tmp/uninstallSAM.<#>.log
   ```
   where <#> is a number; the highest number identifies the most recent log file.

4. To verify which packages were uninstalled, issue the following command:
   - AIX:
     ```bash
     lslpp -l sam*
     ```
   - Linux:
     ```bash
     rpm -qa | grep -E "^src|^rsct|^sam$"
     ```
   Any packages left installed will be listed. If no packages required by other products are left installed, no packages will be listed.
Uninstalling the Base component operations console

This section describes how to uninstall the operations console. An uninstallation program is provided that removes the components that were installed by the installation wizard.

Launching the graphical uninstallation program on Windows

To launch the uninstallation program on Windows, either issue the command <EEZ_INSTALL_ROOT>\uninstall\uninstall.exe at a command prompt or perform the following steps:

1. Open the Control Panel (Start > Control Panel).
2. On the Control Panel, open Add or Remove Programs.
3. On the Add or Remove Programs panel, select IBM Tivoli System Automation for Multiplatforms and click Change/Remove. This brings up the Welcome panel of the uninstallation program.

Launching the graphical uninstallation program on AIX and Linux

To launch the uninstallation program on AIX and Linux, enter the following command in a shell:

<EEZ_INSTALL_ROOT>/uninstall/uninstall

This brings up the Welcome panel of the uninstallation program.

Using the uninstallation program

Before you begin:

- Make backup copies of the following files in the directory <isc_home>/AppServer/profiles/Appsrv01/Tivoli/EEZ to prepare for reusing them after reinstallation:
  - directui-joined-domains.xml
    Contains the domains that you saw most recently in the topology tree.
  - directui-prefs.xml
    Contains user preferences, such as hidden domains and resource filters.
  - directui.properties
    Contains the port on which the operations console listens for events from domains, and SSL information. If you never changed the port from the default and never specified SSL key information, you need not back up the file.
- Before starting the uninstallation of the operations console, make sure that the Integrated Solutions Console server is stopped. For information on how to stop the server, refer to the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide section “Starting and stopping the operations console”.

During uninstallation, you may repeatedly be prompted to confirm that specific files are to be deleted. Make sure that the files should be deleted before confirming the deletion.
Perform the following steps to uninstall the operations console:

1. Launch the uninstallation program as described in the sections above.

2. In the Welcome window, click Next.

3. In the fields in the WebSphere Application Server window, type the user ID and password of the WebSphere administrator, and specify the name of the WebSphere Application Server and the WebSphere Application Server profile. Click Next.

4. The Start Deinstallation window informs you that the preparations for the uninstallation are complete. Click Next.
5. During the uninstallation, information windows like the following inform you of the progress.

![Uninstall IBM Tivoli System Automation for Multiplatforms](image1.png)

6. When the uninstallation is complete, a summary window is displayed. To exit the installation program, click **Done**.
Chapter 5. Uninstalling the Base component for AIX and Linux and the operations console
Chapter 6. Installing the Base component for Windows

Planning for the installation

You can install the Base component for Windows from CD or, if you prefer electronic delivery, download the product archive from the Web after you have purchased IBM Tivoli System Automation.

Base component installation CD

The CD labeled “IBM Tivoli System Automation for Multiplatforms 2.3 Base component all Platforms” contains scripts and software packages for each platform, including Windows, and the corresponding architecture.

To install the Base component for Windows, you use the installation program TSA_Setup.exe which is located in the following directory:

SAM2300Base/Windows

Base component installation archive

The name of the self-extracting archive is C100NML.exe. After extraction, the installation program TSA_Setup.exe is available in the following directory:

SAM2300Base/Windows

Supported languages and locales

The table below shows the combinations of languages and locales that are supported for the Base component for Windows to display translated messages.

Table 20. Languages and locales supported by the Base component for Windows

<table>
<thead>
<tr>
<th>Language</th>
<th>ISO-8859-1</th>
<th>EUC/GBK</th>
<th>SJIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>German</td>
<td>de_DE.ISO-8859-1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>French</td>
<td>fr_FR.ISO-8859-1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Japanese</td>
<td>ja_JP.EUC-JP</td>
<td>win-ja_windows-932</td>
<td></td>
</tr>
</tbody>
</table>

Preparing the system for the installation of the Base component for Windows

Installation prerequisites

The following prerequisites must be met:

- Subsystem for UNIX-based Applications (SUA) must be installed on the system
- The following components of the Utilities and SDKs for SUA must be installed:
  - Base Utilities
For more information, see below.

- 400 MB of free disk space
- **Attention:** The original Subsystem for UNIX-based Applications folder structure must be retained! It is different from that of AIX and Linux. Do not create any additional folders to mimic the folder structure of other UNIX environments. Creating folders that are not present in SUA, for example, the folder `/lib` or `/usr/bin` may interfere with the normal operations of SUA or prevent the installation of the Base component, or both.

### Installing the Subsystem for UNIX-based Applications (required)

Install the Subsystem for UNIX-based Applications (SUA) Windows component from the Windows Server 2003 R2 CD set.

### Installing the Utilities and SDK Package (required)

You can download the “Utilities and SDK for UNIX-based Applications” package at the following location:


To install the package, run the installation program for the package downloaded from Microsoft. During the installation, make the following selections:

- On the Installation Options window of the Setup Wizard, select **Custom Installation**.
- On the Selecting Component window, select:
  - SVR-5 Utilities
  - GNU Utilities
  - GNU SDK
  - Perl

Base Utilities and Base SDK are already selected by default and must not be de-selected. There is no need to install the “Visual Studio Debugger Add-in”.

- On the Security Settings window, keep **Enable setuid behavior for SUA programs** and **Change the default behavior to case sensitive** disabled.

### Verifying the directory structure (required)

Verify that `/lib` is a symbolic link to `/usr/lib` (this is the expected default state after installation):

```bash
/ > ls -lF /lib
lrw-rw-r-- 1 Administrator +Administrators 7 Jan 5 2006 /lib0 -> usr/lib
```

Verify that `/usr/bin` is a symbolic link to `/bin` (this is the expected default state after installation):

```bash
/ > ls -lF /usr/bin
lrw-rw-r-- 1 Administrator +Administrators 6 Jan 5 2006 /usr/bin0 -> ../bin
```
Ensuring that the Administrator UID is set to the correct value

This topic describes the procedures you must perform after installing the Subsystem for UNIX-based Applications to ensure that the administrator UID is set correctly.

The Base component for Windows can only be installed and operated using a Windows Administrator account:
- If the system is not a member of a Windows domain, you must use the local administrator account. By default, the user identifier (UID) of the local administrator account is set to 197108 in Subsystem for UNIX-based Applications. After the installation of the subsystem, you must do this:
  1. Verify that the UID is set to 197108.
  2. If the UID is set to any other value, you must specify the actual UID and GID in the file ctadmins.cfg as described below.
- If the system is a member of a Windows domain, you must use the domain administrator account. After the installation of the subsystem, you must specify the UID and GID of the domain administrator in the file ctadmins.cfg as described below.

Checking the administrator UID

After the Subsystem for UNIX-based Applications is installed, check to which value the UID of the administrator account you are using is set:

1. Log in using the administrator account you will be using to install and operate the Base component.
2. Open a shell, for example, a Korn shell.
3. Issue the command id to retrieve information about your account. The output of this command should look similar to this example:
   ```
   > id
   uid=197108(Administrator) gid=197121(None) groups=197121(None), 5792(+Everyone), 131616(+Administrators), 131617(+Users), 66820(+INTERACTIVE)66827(+Authenticated Users), 66831(+This Organization), 4095(CurrentSession), 66048(+LOCAL), 262154(NT AUTHORITY+NTLM Authentication)
   ```

Results:
- You are using the local administrator account:
  - If the UID is set to 197108, no additional steps are required.
  - If the UID is set to any other value, make a note of the UID and GID displayed in the output and perform the steps described below.
- You are using the domain administrator account: Make a note of the UID and GID displayed in the output and perform the steps described below.

Specifying the administrator UID and GID

Perform these steps to define the administrator UID and GID to the Base component:

1. Create the file /var/ct/cfg/ctadmins.cfg.
2. Add these lines to the file:
   ```
   UID=<your_administrator_UID>
   GID=<your_administrator_GID>
   ```

Verifying and updating TCP/IP configuration files (required)

The SUA TCP/IP stack is realized by Win32 Winsock, which is why the configuration files
hosts
protocol (under UNIX, this file is usually named protocols)
services

are expected in this directory:
%SystemRoot%\system32\drivers\etc

where the SystemRoot environment variable is typically set to C:\WINDOWS on a Windows Server 2003 R2 system.

On a typical UNIX system, the files are located in the /etc directory. Under SUA, the files in the /etc directory are just links to the Windows files as this output of the ls command shows:

```
> ls -lF /etc/hosts
-rw-rw-r-- 1 Administrator +Administrators 44 May 9 12:07 /etc/hosts
> ls -lF /etc/protocols
-rw-rw-r-- 1 Administrator +Administrators 47 May 9 12:07 /etc/protocols
> ls -lF /etc/services
-rw-rw-r-- 1 Administrator +Administrators 47 May 9 12:07 /etc/services
```

The Winsock configuration files must meet the following requirements:

- The Windows/MS-DOS line-end format (rather than UNIX line-end format) must be used.
- All content lines, including the last entry, must have a line ending.

You must make sure that users have the required access rights on the file %SystemRoot%\system32\drivers\etc\services:

- The principal user SYSTEM must have at least read access to the file.
- If you are using the local Administrator with Tivoli System Automation, this user must have read and write access to the file.
- If you are using the Windows domain Administrator with Tivoli System Automation, this user must have read and write access to the file.

Sufficient access rights can best be achieved by granting the local or Windows domain Administrator full access to the file.

To view or change the access rights, you can either use the Windows file explorer or the Windows command cacls. The output of the command will look similar to this example:

```
> cacls services C:\WINDOWS\system32\drivers\etc\services NODE2\Administrator:F
NT AUTHORITY\SYSTEM:R
```

**Updating the DNS or hosts file (required)**

The systems running the Base component for Windows should be included in DNS. If no DNS is available or inclusion in DNS is not desired, the Winsock hosts file on all systems must contain the host names and IP addresses of all remaining systems. Check the hosts files and add systems as necessary.

**Configuring the Subsystem for UNIX-based Applications**

You can perform the configuration before or after installing the Base component for Windows.
This section describes some optional but recommended configuration steps for the Subsystem for UNIX-based Applications. You can perform the configuration before or after installing the Base component for Windows.

In general, it is recommended that you use the following help systems to familiarize yourself with the Subsystem:

- Subsystem for UNIX-based Applications – Getting Started
- Help for Subsystem for UNIX-based Applications

They are available in the Subsystem for UNIX-based Applications folder on the Windows installation media.

**Enabling the syslog daemon**

By default, the system logger daemon (syslog) is not enabled in the Subsystem for UNIX-based Applications. However, most components installed by the Tivoli System Automation Base component are heavily making use of this component in order to log important information for the user.

It is almost impossible to understand the behavior of the Base component if the syslog daemon is not enabled.

To enable the system logger daemon, perform the following steps:

1. Open a Subsystem for Unix-based Application shell, such as the Korn Shell.
2. Change the current working directory:
   ```
   cd /etc/init.d
   ```
3. Open the file syslog for editing (for example, using the vi editor)
4. As described in that file, in the start section, uncomment the lines for starting the syslogd. The result must look like this:
   ```
   ... case $1 in
   start)
   ###
   ### syslogd daemon is disabled by default.
   ### If you want to run syslogd then you
   ### have to uncomment the next few lines.
   ###
   ### ${SYSLOGD}
   [ $? = 0 ] && echo "syslogd started"
   ;;
   stop)
   ...
   ```
5. Save the file.
6. Now the system logger daemon process will be started automatically during system startup. In order to start the process immediately, you have to issue the following command:
   ```
   /usr/sbin/syslogd &
   ```

After the system logger has been configured and started in this way you can find the logs and traces in the file /var/adm/log/messages. You can open this plain text file either by using the vi editor or the less viewer.
Enabling telnet login to Subsystem for UNIX-based Applications (Optional)

After installing the Base component for Windows, an Administrator can use the component either by directly logging on to the Windows system or by opening a standard “Remote Desktop Connection” to open the remote Windows display on the system.

If you want to use telnet sessions for working with the Base component, you must set up the telnet daemon on Windows servers in the same way as you would on Linux and AIX systems.

When the Subsystem for UNIX-based Applications is installed, two different telnet daemons are supported by Windows:

- By default, a user connecting to the Windows server using telnet would open a session to the Win32 subsystem by running the cmd.exe. However, this command prompt cannot be used with the Base component for Windows.
- Which is why it is required to set up the telnet daemon of the Subsystem for UNIX-based Applications. To set up the telnet daemon, follow the instructions provided in the SUA documentation Help for Subsystem for UNIX-based Applications, in chapter “Starting the Subsystem for UNIX-based Applications telnetd and rshd daemons”.

Installing the Base component for Windows

Perform the following steps:

1. Log in on the Windows system with the appropriate administrator account (see “Ensuring that the Administrator UID is set to the correct value” on page 49).
2. Launch the installation wizard (TSA_Setup.exe). When the installation wizard is ready, the initial wizard panel appears:
3. Select the language in which the text on the installation wizard panels is to appear and click OK. The language in which the Base component is installed is derived from the system’s locale setting.

4. Read the information on the Introduction panel and click Next.

5. Carefully read the terms of the license agreement. Make sure to also read the non-IBM terms by clicking Read non-IBM terms.
To accept the terms of the license agreement, select I accept both the IBM and the non-IBM terms and click Next.

6. Wait while the requirements check is being performed.

7. If the check was not successful, click Cancel to exit, correct the cause of the problem, and restart the installation. If the check was successful, click Next.

8. The Base component program files will be installed in the Windows SUA root directory, which is automatically discovered on the system. On the Choose Install Folder panel, you can specify the directory where the uninstallation program and the product documentation are to be installed:
Specify a directory or accept the default and click Next.

9. On the Choose Shortcut Locations panel, make your selections and click Next.

10. Leave the check box selected to install the documentation.
11. Specify the password of the administrator account that you are using to install and operate the Base component. Click Next.

12. Review the information on the Pre-Installation Summary panel and click Install to start the installation.
A number of transient panels appear while the Base component is being installed.
13. On the Installation Complete panel, click **Done** to exit the installation wizard.

**Note:** After the installation of the Base component for Windows, you find the following entries on the Add or Remove Programs panel in addition to the entry **Tivoli SA MP Base**:
- RSCTMM
- RSCTNLV
- SAMMM
- SAMNLV
These programs are part of the Base component for Windows, be sure not to remove them separately.

Verifying the installation

To verify that the installation was successful, do this:

1. Open the IBM Tivoli System Automation Shell (Start > All Programs > Tivoli SA MP Base > IBM Tivoli System Automation Shell)
2. Check that the System Resource Controller (SRC) is running by checking the output of the command:
   ```
   ps -efi -Xunix | grep srcmstr
   ```
   If the SRC is not running, start it from the Windows Services Manager: Locate the entry System Resource Controller and start it again.

Default profile changes made to your default profile

During installation of the Base component for Windows some changes are made to the file /etc/profile.lcl in order to:

- Automatically set up the correct RSCT Management scope for the Administrator account when the IBM Tivoli System Automation Shell is being opened
- Use the correct code page when the system is set up to use the German or French locale.

This is an excerpt from the /etc/profile.lcl file after the installation of the Base component for Windows is complete:

```bash
# TSAWin
export CT_MANAGEMENT_SCOPE=2

# For supported Western European locales, set the appropriate codepage
if [ "$LANG" = "de_DE.ISO-8859-1" ]
then
```

Chapter 6. Installing the Base component for Windows  59
License installation

The Base component on Windows supports only one type of license. A Try&Buy license is not available.

The license key is part of the installation media and is automatically enabled during installation. If the license key was not available at installation time for some reason, it will not be possible to add a resource to a resource group, which means that it will not be possible to automate it.

You can use the `samlicm` command found in `/usr/sbin/rsct/bin` to install a valid license key at any time later:
1. Open an IBM Tivoli System Automation Shell.
2. Issue the command `samlicm -i <fully qualified file name of key file>`

Setting up the Windows firewall

You must set up the Windows firewall to protect the automation domain from being accessed by unauthorized users or programs connecting from systems which are not defined members of the domain.

To set up the Windows firewall, perform these steps on each node of the domain:
1. Click **Start > Control Panel > Windows Firewall**.
2. Enable the firewall by selecting the radio button **On**. This protects this Windows system from all outside network traffic.
3. To make the Tivoli System Automation domain operational, you must add firewall exceptions for all trusted systems within the automation domain:
   On the **Exception** tab, add the ports listed below. For each port that you add, click **Change scope** and add the IP addresses of all other nodes in the automation domain to the field **Custom list**.

The following ports must be opened in this way on all nodes of the automation domain:

*Table 21. Windows firewall: Required port exceptions*

<table>
<thead>
<tr>
<th>Name</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAGS</td>
<td>12348</td>
<td>UDP</td>
</tr>
<tr>
<td>HATS</td>
<td>12347</td>
<td>UDP</td>
</tr>
<tr>
<td>RMC</td>
<td>657</td>
<td>UDP</td>
</tr>
<tr>
<td>RMC</td>
<td>657</td>
<td>TCP</td>
</tr>
</tbody>
</table>
Chapter 7. Post-installation tasks for the Base component for Windows

Configuring a non-English environment for the Base component for Windows

The Base component for Windows supports the following languages:
- English
- German
- French
- Japanese

If you are using the Base component for Windows in a non-English environment, either stop and restart the System Resource Controller (SRC) Windows service or reboot the system after the installation of the Base component for Windows is complete. To stop and restart the SRC Windows service, use the following commands:

1. Stop all subsystems under the control of System Resource Controller by issuing `stopsrc -a`
2. Stop and re-start the System Resource Controller Windows service
3. Restart the ctrmc subsystem by issuing `rmctrl -s`

To use a Japanese locale, the native Windows system where the Base component is installed must be a Japanese Windows system.

Opening a IBM Tivoli System Automation Shell from the Windows desktop

If you log in at the Windows desktop directly or via a Windows Remote Desktop connection and open a IBM Tivoli System Automation Shell from the Windows desktop, perform the following steps:

<table>
<thead>
<tr>
<th>IBM Tivoli System Automation Shell property</th>
<th>German</th>
<th>French</th>
<th>Japanese</th>
</tr>
</thead>
<tbody>
<tr>
<td>Font</td>
<td>Lucida Console</td>
<td>Lucida Console</td>
<td>default</td>
</tr>
<tr>
<td>Code page</td>
<td>28591</td>
<td>28591</td>
<td>932</td>
</tr>
</tbody>
</table>

To view the currently active locale, use the `locale` command. To set the locale, use the `export LANG=<locale>` command. To change the font, use the Properties menu item of the IBM Tivoli System Automation Shell window and switch to the Font tab. To view the active code page, use the `chcp` command. To change the active code page, use the `chcp <codepage_number>` command.
Opening a telnet session from a Windows command prompt

If you use the `telnet` command from a local Windows command prompt in order to log in to a Windows server where the Base component is installed, perform the following steps:

**Table 23. Windows command prompt properties**

<table>
<thead>
<tr>
<th>Windows command prompt property</th>
<th>German</th>
<th>French</th>
<th>Japanese</th>
</tr>
</thead>
<tbody>
<tr>
<td>Font</td>
<td>Lucida Console</td>
<td>Lucida Console</td>
<td>default</td>
</tr>
<tr>
<td>Code page</td>
<td>28591</td>
<td>28591</td>
<td>932</td>
</tr>
</tbody>
</table>

Then, open the telnet session from the command prompt and perform the following steps:

**Table 24. Telnet session properties**

<table>
<thead>
<tr>
<th>Telnet session property</th>
<th>German</th>
<th>French</th>
<th>Japanese</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locale</td>
<td>de_DE.ISO-8859-1</td>
<td>fr_FR.ISO-8859-1</td>
<td>win-ja_JP.windows-932</td>
</tr>
</tbody>
</table>

Opening a remote session using a terminal

If you will be using a terminal to log in on a Windows server where the Base component is installed, perform the following steps:

**Table 25. Session properties**

<table>
<thead>
<tr>
<th>Session property</th>
<th>German</th>
<th>French</th>
<th>Japanese</th>
</tr>
</thead>
<tbody>
<tr>
<td>Character set translation on received data</td>
<td>ISO-8859-1 (Latin-1, Western Europe)</td>
<td>ISO-8859-1 (Latin-1, Western Europe)</td>
<td>Shift_JIS</td>
</tr>
</tbody>
</table>

Once you have connected to the Windows SUA environment, verify the following properties:

**Table 26. Session properties**

<table>
<thead>
<tr>
<th>Shell property</th>
<th>German</th>
<th>French</th>
<th>Japanese</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locale</td>
<td>de_DE.ISO-8859-1</td>
<td>fr_FR.ISO-8859-1</td>
<td>win-ja_JP.windows-932</td>
</tr>
</tbody>
</table>
Chapter 8. Uninstalling the Base component for Windows

Note: After a successful installation, background processes still run for approximately 5 to 10 minutes before the installation is complete. Wait at least 10 minutes after a successful installation before performing an uninstallation.

You use an uninstallation program to uninstall the Base component for Windows. To launch the wizard, use one of the following approaches:

- From Windows Control Panel, do this:
  1. Open Add or Remove Programs in Control Panel.
  2. Click Change/Remove.
  3. Click Tivoli SA MP Base.
  4. Click Remove.
- Click Start > All Programs > Tivoli SA MP Base > Uninstall Tivoli SA MP Base

The uninstallation wizard comprises these panels:

1. On the first panel, click Uninstall to start the uninstallation.

2. While the uninstallation is being performed, panels are shown that inform you of the progress:
3. When the uninstallation is complete, click **Done** to close the wizard.
Chapter 8. Uninstalling the Base component for Windows

All items were successfully uninstalled.
Chapter 9. Installing and uninstalling service

Installing service

Installing service means applying corrective service fix packs to release 2.3 of IBM Tivoli System Automation for Multiplatforms or upgrading the software release level from release 2.3. Such service fix packs are referred to as product fix packs in this guide. Product fix packs are available for the Base component including the operations console.

Product fix packs are delivered in the following formats:

- For Linux: Archives in TAR-format
- For AIX: Archives in TAR-format or self-extracting archives (operations console only)
- For Windows: Self-extracting archives

Where to obtain fix packs

Read the release notes to find out which fix packs are required for a release update. To obtain a copy of the release notes, go to the IBM Tivoli System Automation for Multiplatforms home page and click Technical Documentation. The IBM Tivoli System Automation home page is located at:


Archives for product fix packs can be downloaded from the IBM Tivoli System Automation support site at:


Download the archive to a temporary directory. Typically, one archive is available for each platform. For information about the naming conventions that apply to product fix pack archives, refer to "Archive naming conventions."

Archive naming conventions

The archives for product fix packs for the Base component of IBM Tivoli System Automation and the operations console have the following syntax:

2.3.0-TIV-SABASE-<platform>-FP<fix_pack_number>.<archive_type> containing the service for the Base component, and

2.3.0-TIV-SAE2E-<platform>-FP<fix_pack_number>.<archive_type> containing the service for the operations console.

where

- <platform> represents the platform on which IBM Tivoli System Automation for Multiplatforms is installed
- <fix_pack_number> represents the fix pack number
- <archive_type> is either tar, bin, or exe

Example:

This is the tar archive that is used to install fix pack 1 for IBM Tivoli System Automation for Multiplatforms 2.3 on AIX platforms:

2.3.0-TIV-SABASE-AIX-FP0001.tar
Installing service for the Base component

The tables below list the archive files you can download for applying service for the Linux, AIX, and Windows operating systems:

Usage instructions for the platform-specific archives

Linux:

Table 27. Archive for Linux platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SABASE-LIN-&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required. Use the <code>tar -xf</code> command to extract the archive. This is where you find the install script <code>installSAM</code> after extracting the archive: <code>SAM23&lt;maintenance_level&gt;Base/installSAM</code></td>
</tr>
</tbody>
</table>

AIX:

Table 28. Archive for AIX platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SABASE-AIX-&lt;fix_pack_number&gt;.tar</td>
<td>Use the <code>tar -xf</code> command to extract the archive. This is where you find the install script <code>installSAM</code> after extracting the archive: <code>SAM23&lt;maintenance_level&gt;Base/installSAM</code></td>
</tr>
</tbody>
</table>

Windows:

Table 29. Archive for Windows platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SABASE-WIN-&lt;fix_pack_number&gt;.exe</td>
<td>The archive is self-extracting. This is where you find the update installation wizard after extracting the archive: <code>SAM23&lt;maintenance_level&gt;Base\Windows\update.exe</code></td>
</tr>
</tbody>
</table>

Steps for installing service for the Base component

Before you begin:

- Installing service means upgrading IBM Tivoli System Automation from release 2.3. Therefore, release 2.3 must have been installed before any service can be applied.
- Product fix packs are always cumulative.
- For AIX and Linux, you must have root authority to install a product fix pack. For Windows, administrator authority is required.
- When you have downloaded the archives from the IBM Tivoli System Automation for Multiplatforms support site (see "Where to obtain fix packs" on page 67), unpack the product fix pack archive to a temporary directory. For information about how to unpack the archive for your platform, refer to "Usage instructions for the platform-specific archives."
- Before performing the steps below, check the release notes for additional or deviating installation instructions.
- For installing service on AIX or Linux platforms:
- Back up your system configuration before installing service. For information on how to do this, refer to the IBM Tivoli System Automation for Multiplatforms Base Component Administrator's and User's Guide section "Automation Policy Management".
- To minimize downtime, you can perform a prerequisites check before starting the installation (for more information, see "Performing the prerequisites check" on page 9).

Perform the following steps on each node in the peer domain:

1. Check if any resources are online on the node you want to service:
   - If resources are online and must be kept available, exclude the node from automation using the command
     `samctrl -u a <node>`
     IBM Tivoli System Automation for Multiplatforms stops the resources on the node and, if possible, restarts them on a different node in the peer domain.
   - If the resources need not be kept available during service, bring the resource groups offline.

2. Stop the node from another node in the domain, and verify that it is stopped:
   `stoprpnode <node>; lsrpnode`

3. After receiving the archives, extract them. They create a directory structure with root directory SAM23mf/Base, where mf stands for modification level and fix level.

4. Do this:
   **AIX, Linux:**
   Install the service fix pack with the `installSAM` script. For detailed information about the script, refer to "Installing the Base component for AIX and Linux" on page 9.

   **Windows:**
   a. Change to the directory in which the update installallation wizard is located. For information on where to find the update wizard, see Table 29 on page 68
   b. Launch the update installer. The update installer for fix packs is named update.
   c. Follow the instructions on the wizard panels to install the product fix pack.

5. Start the node:
   `startrpnode <node>`

6. If you had excluded the node in step 2, include the node in automation again using the command
   `samctrl -u d <node>`

7. If you require the resource groups to be online, bring the resource groups online. Otherwise delay this step until after the last node in the peer domain has been serviced.

8. After all nodes have been serviced, perform the steps described in "Completing the migration" on page 15. This ensures that the changes become effective in the entire domain and the correct version is shown.
Installing service for the operations console

These are the archives for applying service for the operations console.

Usage instructions for the platform-specific archives

Windows:

Table 30. Windows platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-WIN-&lt;fix_pack_number&gt;.exe</td>
<td>The archive is self-extracting. This is where you find the update installer program after unpacking the archive: EEZ23&lt;maintenance_level&gt;E2EWindows/Windows/update.exe</td>
</tr>
</tbody>
</table>

AIX:

Table 31. AIX platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-AIX-&lt;fix_pack_number&gt;.bin</td>
<td>The archive is self-extracting. This is where you find the update installer program after unpacking the archive: EEZ23&lt;maintenance_level&gt;E2EAIX/AIX/update</td>
</tr>
</tbody>
</table>

Linux on IBM System x:

Table 32. Linux on IBM System x

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-I386-&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory. This is where you find the update installer program after unpacking the archive: EEZ23&lt;maintenance_level&gt;E2EI386/i386/update</td>
</tr>
</tbody>
</table>

Linux on POWER:

Table 33. Linux on POWER

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-PPC-&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory. This is where you find the update installer program after unpacking the archive: EEZ23&lt;maintenance_level&gt;E2EPPC/ppc/update</td>
</tr>
</tbody>
</table>
Linux on System z:

Table 34. Linux on System z

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-S390-&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required.</td>
</tr>
<tr>
<td></td>
<td>Use the tar -xf command to extract the files to a temporary directory.</td>
</tr>
<tr>
<td></td>
<td>This is where you find the update installer program after unpacking the archive:</td>
</tr>
<tr>
<td></td>
<td>EEZ23&lt;maintenance_level&gt;E2ES390/s390/update</td>
</tr>
</tbody>
</table>

Installing product fix packs for the operations console

- When you have downloaded the archives from the IBM Tivoli System Automation for Multiplatforms support site (see “Where to obtain fix packs” on page 67), unpack the product fix pack archive to a temporary directory. For information about how to unpack the archive for your platform, refer to “Usage instructions for the platform-specific archives” on page 70.
- Before performing the subsequent steps, check the release notes for additional or deviating installation instructions.
- Change to the directory in which the update wizard program is located. For information on where to find the update wizard program, refer to “Usage instructions for the platform-specific archives” on page 70.
- Launch the update wizard. The update wizard for fix packs is named update. When the wizard is launched successfully, the Welcome panel appears.
- Follow the instructions on the wizard panels to install the product fix pack.

Uninstalling service

To uninstall a fix pack, you need to uninstall the complete product as described in the following sections:

- To uninstall the Base component for AIX or Linux, follow the instructions in “Uninstalling the Base component for AIX and Linux” on page 41.
- To uninstall the Base component for Windows, follow the instructions in Chapter 8, “Uninstalling the Base component for Windows,” on page 63.
- To uninstall the operations console, follow the instructions in “Uninstalling the Base component operations console” on page 42.

After the uninstallation is complete, you can reinstall IBM Tivoli System Automation for Multiplatforms and the required service level (fix pack level).
Part 2. End-to-End Automation Management component

Chapter 10. Installing the End-to-End Automation Management component .............. 75
Planning for installation .............. 75
Packaging .............. 75
- Product CD and WebSphere Application Server Upgrade CD .............. 75
- Electronic distribution .............. 76
Product features and DB2 setup options .............. 78
DB2 setup options .............. 79
Product requirements .............. 79
- Supported operating systems .............. 79
- Middleware software requirements .............. 81
- Supported Web browsers .............. 81
- Hardware requirements .............. 82
Security concepts .............. 83
- Security considerations .............. 83
User management .............. 84
Installing the middleware software .............. 84
- Contents of the middleware software CDs .............. 84
Installing a DB2 server .............. 84
- DB2 server requirements .............. 84
- DB2 server installation .............. 85
Post-installation tasks for remote DB2 setup .............. 86
Installing WebSphere Application Server .............. 87
- WebSphere Application Server 6.1.0.9 requirements .............. 87
- Installing WebSphere Application Server 6.1.0.0 .............. 88
- Upgrading WebSphere Application Server 6.1.0.0 .............. 88
Preparing for the installation of the End-to-End Automation Management component .............. 89
- Collecting the information you need to provide during installation .............. 89
- Installation directory and Tivoli Common Directory .............. 90
- Installation parameters for DB2 .............. 91
- WebSphere Application Server installation parameters .............. 93
- IBM Tivoli Enterprise Console connection configuration data .............. 94
- Name of the end-to-end automation domain .............. 94
WebSphere Application Server user ID for the end-to-end automation engine .............. 94
System Automation Administrator User ID .............. 94
What the installation CD contains .............. 95
Languages and locales supported by the End-to-End Automation Management component .............. 95
- Languages supported on Linux systems .............. 95
- Languages and locales supported on AIX systems .............. 96
Installation prerequisites .............. 96
Installing the End-to-End Automation Management component using the installation wizard .............. 97
Installing the End-to-End Automation Management component in silent mode .............. 110
Verifying the installation .............. 111
- Automation manager .............. 111
- End-to-end automation database .............. 111
- Automation J2EE Framework .............. 111
- Verifying that DB2 accepts WebSphere Application Server requests .............. 112
- Automation engine .............. 112
- Operations console .............. 112
Post-installation tasks .............. 114
- Modifying the LTPA settings .............. 114
- Modifying the HTTP session timeout .............. 114
- Configuring how many users can connect to the automation manager using the operations console .............. 115
Chapter 11. Upgrading the End-to-End Automation Management component from release 2.2 .............. 117
Chapter 12. Configuring the end-to-end automation manager .............. 119
- Invoking the end-to-end automation manager configuration dialog .............. 119
- Using the task launcher .............. 119
- Displaying online help .............. 120
End-to-end automation manager basic configuration .............. 121
- Domain tab .............. 122
- Command shell tab .............. 123
- User credentials tab .............. 124
- Security tab .............. 125
- Logger tab .............. 126
- Saving the basic configuration .............. 128
Configuring high availability for the end-to-end automation manager .............. 128
- Domain setup tab .............. 129
- Automation manager tab .............. 130
- Policy pool tab .............. 131
- WebSphere tab .............. 132
- DB2 tab .............. 133
- Saving the high-availability configuration .............. 134
- Restoring an existing high-availability configuration .............. 134
- Replicating the configuration files .............. 134
- Setting up the domain .............. 135
- Removing the domain .............. 135
- Defining the automation policy for the end-to-end automation manager .............. 136
- Removing the automation policy for the end-to-end automation manager .............. 137
Chapter 13. Installing and uninstalling service .............. 139
Installing service .............. 139
- Where to obtain fix packs .............. 139
- Archive naming conventions .............. 139

© Copyright IBM Corp. 2006, 2007
Chapter 14. Uninstalling the End-to-End Automation Management component

Launching the graphical uninstallation program on Windows . . . . . . 143
Launching the graphical uninstallation program on AIX and Linux . . . . . . 143
Using the uninstallation program . . . . . . 143
Chapter 10. Installing the End-to-End Automation Management component

Planning for installation

This chapter contains the information you need for preparing the installation of the End-to-End Automation Management component.

Packaging

The End-to-End Automation Management component can be ordered from IBM as media pack or downloaded from an IBM software distribution download site.

Product CD and WebSphere Application Server Upgrade CD

When you order the End-to-End Automation Management component on CD, you receive the following CDs:

- One product CD for each operating system on which the product can be installed. You use the product CD to install the End-to-End Automation Management component.
- One WebSphere Application Server Upgrade CD for each operating system on which the product can be installed. You use the upgrade CD to bring WebSphere Application Server to the version level required for the End-to-End Automation Management component.

For information about the middleware software CDs that are shipped with the End-to-End Automation Management component, refer to “Contents of the middleware software CDs” on page 84.

Product CD: The following table lists the versions of the product CDs that are available for the End-to-End Automation Management component. To install the product, you use the installation wizard file listed in the right column of the table.

Table 35. Product CD versions

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Product CD label</th>
<th>Installation wizard file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 End-to-End component for Windows</td>
<td>EEZ2300E2EWindows\Windows\setup.exe</td>
</tr>
<tr>
<td>AIX</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 End-to-End component for AIX</td>
<td>EEZ2300E2EAI/X/setup.bin</td>
</tr>
<tr>
<td>Linux on System x</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 End-to-End component for Linux on System x</td>
<td>EEZ2300E2E1386/1386/setup.bin</td>
</tr>
<tr>
<td>Linux on POWER</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 End-to-End component for Linux on POWER</td>
<td>EEZ2300E2EPPC/ppc/setup.bin</td>
</tr>
</tbody>
</table>
Table 35. Product CD versions (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Product CD label</th>
<th>Installation wizard file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux on System z</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 End-to-End component for Linux on System z</td>
<td>EEZ2300E2ES390/s390/setup.bin</td>
</tr>
</tbody>
</table>

WebSphere Application Server upgrade CD: The following table lists the available versions of the WebSphere Application Server upgrade CDs.

Table 36. WebSphere Application Server upgrade CD versions

<table>
<thead>
<tr>
<th>Operating system</th>
<th>CD label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 WAS 6.1 upgrade for Windows</td>
</tr>
<tr>
<td>AIX</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 WAS 6.1 upgrade for AIX</td>
</tr>
<tr>
<td>Linux on System x</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 WAS 6.1 upgrade for Linux on System x</td>
</tr>
<tr>
<td>Linux on POWER</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 WAS 6.1 upgrade for Linux on POWER</td>
</tr>
<tr>
<td>Linux on System z</td>
<td>IBM Tivoli System Automation Multiplatforms V2.3.0 WAS 6.1 upgrade for Linux on System z</td>
</tr>
</tbody>
</table>

Electronic distribution

You can also obtain the End-to-End Automation Management component through electronic distribution. In this case, you can download the deliverables from a URL you receive after purchasing the product.

The following tables list the archives that you need to download for each platform to install the WebSphere Application Server upgrade, which is required for running the End-to-End Automation Management component, and the product itself.

Archives: The following tables list the archives that you need for installing the WebSphere Application Server upgrade and the product itself.

Windows:

Table 37. Archives for Windows platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1069ML.exe</td>
<td>This is the archive you use to install the product. The archive is self-extracting. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
<tr>
<td>C106HML.exe</td>
<td>The self-extracting archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
</tbody>
</table>
### AIX:

**Table 38. Archives for AIX platforms**

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C106AML.bin</td>
<td>This is the archive you use to install the product. The archive is self-extracting. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
<tr>
<td>C106JML.bin</td>
<td>The self-extracting archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
</tbody>
</table>

### Linux on System x:

**Table 39. Archives for Linux on System x**

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C106BML.tar</td>
<td>This is the archive you use to install the product. For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
<tr>
<td>C106JML.tar</td>
<td>The archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
</tbody>
</table>

### Linux on POWER:

**Table 40. Archives for Linux on POWER**

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C106CML.tar</td>
<td>This is the archive you use to install the product. For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
<tr>
<td>C106KML.tar</td>
<td>The archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
</tbody>
</table>
Table 41. Archives for Linux on System z

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C106DML.tar</td>
<td>This is the archive you use to install the product. For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files to a temporary directory. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
<tr>
<td>C106LML.tar</td>
<td>The archive contains the files that you need for installing the WebSphere Application Server upgrade. After extraction, the directory structure is identical to that on the corresponding CD.</td>
</tr>
</tbody>
</table>

**Product features and DB2 setup options**

The two major subcomponents of the End-to-End Automation Management component, namely, the end-to-end automation manager and the operations console are installed on the same node and run in the same instance of WebSphere Application Server. During the installation of the End-to-End Automation Management component, the automation J2EE framework, the operations console, and the resource adapters are deployed to an existing instance of WebSphere Application Server. Typically, the name of this server instance is “server1”.

The following figure depicts the setup of the End-to-End Automation Management component.
For more information about the subcomponents of the End-to-End Automation Management component, refer to the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide section “Components of end-to-end automation management”.

**DB2 setup options**

When planning for the installation of the End-to-End Automation Management component, you must decide how you want to set up DB2 for the DB2 database that is required for the End-to-End Automation Management component. You have the following options:

**Local DB2 setup**

The DB2 server is installed and runs on the same node on which the End-to-End Automation Management component is installed.

**Remote DB2 setup**

The DB2 server is installed and runs on a node other than that on which the End-to-End Automation Management component is installed. In this case, you need to install a DB2 JDBC driver on the end-to-end automation management node.

**Product requirements**

The following sections list the software and hardware requirements for the End-to-End Management component.

**Supported operating systems**

The following table lists the operating systems that are supported for the End-to-End Automation Management component:

---

*Figure 4. Setup of the End-to-End Automation Management component*
### Table 42. Supported operating systems

<table>
<thead>
<tr>
<th>Operating system</th>
<th>System x&lt;sup&gt;1&lt;/sup&gt;</th>
<th>System i</th>
<th>System p</th>
<th>System z</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 5.2 (AIX 5L Version 5.2) ML 5</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIX 5.3 (AIX 5L Version 5.3) ML 4&lt;sup&gt;1&lt;/sup&gt;</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 9 (32 bit)&lt;sup&gt;2&lt;/sup&gt;</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 9 (64 bit)&lt;sup&gt;3&lt;/sup&gt;</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
<tr>
<td>SUSE SLES 10 (32 bit)&lt;sup&gt;2&lt;/sup&gt;</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSE SLES 10 (64 bit)&lt;sup&gt;3&lt;/sup&gt;</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
<tr>
<td>Red Hat RHEL 4.0 AS (32 bit)&lt;sup&gt;2&lt;/sup&gt;</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat RHEL 4.0 AS (64 bit)&lt;sup&gt;3&lt;/sup&gt;</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
<tr>
<td>Red Hat RHEL 5.0 AS (32 bit)&lt;sup&gt;2&lt;/sup&gt;</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Hat RHEL 5.0 AS (64 bit)&lt;sup&gt;3&lt;/sup&gt;</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

**Notes:**

1. IBM System x with IA32, EM64T, or AMD64 architecture.
   Any other systems with IA32, EM64T, or AMD64 architecture are also supported.
   Systems with IA64 architecture are not supported.
2. The following Linux kernel architectures are supported for running with 32 bit:
   - x86 on IBM System x
3. The following Linux kernel architectures are supported for running with 64 bit:
   - ppc64 on IBM System i and IBM System p
   - s390x on IBM System z is supported for some distributions
4. APAR IY65979 must be installed.
**Middleware software requirements**

The following middleware software must be installed on the system on which the End-to-End Automation Management component will run, before the component itself can be installed:

- DB2: A DB2 server for a local DB2 setup or a DB2 JDBC driver for a remote DB2 setup
- WebSphere Application Server

**Software prerequisites for a local DB2 setup:** If you are using a local DB2 setup, the end-to-end automation management database and the database tables are created by the installation program during the installation of the End-to-End Automation Management component. Before you can install the component, one of the following IBM DB2 UDB versions must be manually installed on the system on which the End-to-End Automation Management component will run:

- IBM DB2 UDB, Version 9.1, which is bundled with IBM Tivoli System Automation for Multiplatforms, Version 2.3
- IBM DB2 UDB Enterprise Server Edition, Version 8.2.3 (equivalent to V8R1 FixPack 10)

**Note:** When you want to use a local DB2 setup but do not want the installation program to create the end-to-end automation management database and the database tables, just select the radio button for remote DB2 setup (**IBM DB2 UDB on different system (remote)**) on the Database Server window of the installation program. If you make this selection, the installation wizard will neither create the database nor any tables and you are free to set up the database manually as you would for remote setup.

**Software prerequisites for a remote DB2 setup:** Before you can install the automation manager and the operations console, the following software prerequisites must be manually installed:

- One of the following IBM DB2 UDB server versions must be installed on a system other than end-to-end automation management node:
  - IBM DB2 UDB, Version 9.1, which is bundled with IBM Tivoli System Automation for Multiplatforms, Version 2.3
  - IBM DB2 UDB Enterprise Server Edition, Version 8.2.3 (equivalent to V8R1 FixPack 10)
- Additionally, a DB2 JDBC driver must be installed on the end-to-end automation management node:
  1. Copy the DB2 JDBC driver files from the Java directory of your DB2 server to the system where you install the End-to-End Automation Management component. The name of the location/directory is at your discretion.
  2. Make that location/directory accessible to WebSphere Application Server and the end-to-end automation installation program.

**Supported Web browsers**

The operations console is the user interface of the End-to-End Automation Management component. It is displayed in a Web browser that connects to the WebSphere Application Server on which the operations console is running. The Web browser may run on an arbitrary system.

The following Web browsers are supported:

- Microsoft Internet Explorer V6.0 SP1
- Mozilla V1.7.8
- Firefox V1.5
For information on how the Web browser must be configured, refer to the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide section “Configuring your Web browser”.

**Hardware requirements**

The following sections describe the hardware requirements for the End-to-End Automation Management component. The description does not cover the hardware requirements that need to be satisfied for installing and running the required middleware software. For more information on hardware requirements for the required middleware software, refer to “Installing the middleware software” on page 84.

**Memory:** 1.5 GB is required on the server on which the End-to-End Automation Management component is installed (for WebSphere Application Server and the End-to-End Automation Management component).

**TCP/IP connectivity:** The End-to-End Automation Management component consists of various components that may run on one or several systems. For example:

- When you use a local DB2 setup, the automation manager, the operations console, and the DB2 server run on the same system (single-node setup).
- When you use a remote DB2 setup, the End-to-End Automation Management component and the DB2 server run on separate systems (multi-node setup).

Be sure that TCP/IP connections can be established between the following components:

- the WebSphere Application Server that is running the automation J2EE framework, the resource adapters, and the operations console
- the DB2 server

**Disk space requirements:**

*Disk space requirements on Windows systems:* The following table lists the disk space requirements for the End-to-End Automation Management component on Windows systems. Note that the table does not include the space required for the installation of the middleware software.

<table>
<thead>
<tr>
<th>Description</th>
<th>Default directory</th>
<th>Disk space</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-to-End Automation Management component installation directory</td>
<td>C:\Program Files\IBM\tsamp\eez</td>
<td>100 MB</td>
</tr>
<tr>
<td>Automation manager and operations console deployed in WebSphere Application Server</td>
<td>C:\Program Files\IBM\WebSphere\AppServer</td>
<td>50 MB</td>
</tr>
<tr>
<td>DB2 database</td>
<td>C:\DB2</td>
<td>120 MB</td>
</tr>
</tbody>
</table>
Table 43. Disk space requirements on Windows systems (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Default directory</th>
<th>Disk space</th>
</tr>
</thead>
</table>
| Temporary disk space needed for installation and installation log and response files | The value of the system variable %TEMP%  
Typically, this is:  
C:\Documents and Settings\Administrator\Local Settings\Temp | 125 MB     |
| Configuration file directory and policy pool directory of the End-to-End Automation Management component | C:\Program Files\IBM\tsamp\eez\cfg  
C:\Program Files\IBM\tsamp\eez\policyPool | 1 MB       |
| Tivoli Common Directory                                                   | C:\Program Files\IBM\tivoli\common\eez | 250 MB     |
| Installer registry                                                        | The Zero G Registry resides in the hidden directory:  
C:\Program Files\Zero G Registry\com.zerog.registry.xml | 10 KB      |

Disk space requirements on AIX and Linux systems: The following table lists the disk space requirements for the End-to-End Automation Management component on AIX and Linux systems. Note that the table does not include the space required for the installation of the middleware software.

Table 44. Disk space requirements on AIX and Linux systems

<table>
<thead>
<tr>
<th>Description</th>
<th>Default directory</th>
<th>Disk space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation directory of the End-to-End Automation Management component</td>
<td>/opt/IBM/tsamp/eez</td>
<td>110 MB</td>
</tr>
</tbody>
</table>
| Automation manager and operations console deployed in WebSphere Application Server | AIX: /usr/IBM/WebSphere/AppServer  
Linux: /opt/IBM/WebSphere/AppServer | 30 MB       |
| DB2 database                                                                | -db2inst1                                                                        | 120 MB     |
| Temporary disk space needed for installation and installation log and response files | /tmp                                                                            | 125 MB     |
| Configuration file directory and policy pool directory of the End-to-End Automation Management component | /etc/opt/IBM/tsamp/eez/cfg  
/etc/opt/IBM/tsamp/eez/policyPool | 1 MB       |
| Tivoli Common Directory                                                   | /var/ibm/tivoli/common/eez                                                      | 250 MB     |
| Installer registry                                                        | /var/.com.zerog.registry.xml                                                     | 5 KB       |

Security concepts

The following sections describe the security concepts for the End-to-End Automation Management component.

Security considerations

In a local DB2 setup, in which the End-to-End Automation Management component and the external components needed for running (WebSphere Application Server and DB2) are installed on the same system, you do not need to secure the connections between these components over SSL.
The external connections that will be established between the components listed below, however, should be secured over SSL, especially if the external components are running in different security domains that are separated by firewalls.

External connections will be established between the following components (the default port numbers are given in brackets):

- The connection between the automation engine and the automation adapters (port 2001).
- The connection between the automation adapters and the automation engine (port 2002). Note that SSL is not supported for this connection.
- The connection between the Web browsers in which the operations console is displayed and Integrated Solutions Console (HTTP port 9060, HTTPS port 9043).

**User management**

For information on how user IDs and passwords for end-to-end automation management are managed, refer to the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide chapter “Managing users”.

**Installing the middleware software**

Depending on the setup type you choose, middleware software has to be installed on one or more systems before the End-to-End Automation Management component can be installed.

- For information on possible setup types, refer to “DB2 setup options” on page 79
- For information on the required middleware software for each system, refer to “Middleware software requirements” on page 81

**Contents of the middleware software CDs**

The middleware software CDs that are shipped with the end-to-end automation management product CDs contain the following software products:

- IBM DB2 UDB Version 9.1 Enterprise Server Edition (DB2 server)
- The 32-bit version of IBM WebSphere Application Server Base Version 6.1

**Notes:**

1. IBM Tivoli System Automation for Multiplatforms only supports the 32-bit version of WebSphere Application Server.
2. In addition to a WebSphere Application Server 6.1 CD for every supported platform, a WebSphere Application Server 6.1.0 upgrade CD is available for each supported platform. The upgrade CD is needed for bringing WebSphere Application Server to the required product level.
3. WebSphere Application Server 6.1 Network Deployment is not supported.
4. Please note that the IBM Tivoli Directory Server is not contained on the middleware software CDs.

**Installing a DB2 server**

**DB2 server requirements**

Use the following publications to find out which requirements need to be met for installing and running a DB2 server:

- IBM DB2 Universal Database - Quick Beginnings for DB2 Servers (GC09-4836)
• IBM DB2 Universal Database - Release Notes - Version 9

The latest versions of these publications are available on the IBM DB2 UDB Web site:

www.ibm.com/software/data/db2/udb/support/

You find the link to the PDF manuals in the Other resources section on the Web page.

In addition, check for the latest system requirements at

www.ibm.com/software/data/db2/udb/sysreqs.html

The DB2 release notes can also be found on the CD labeled IBM DB2 Universal Database Enterprise Server Edition Version 9.1 for your platform. Make sure that all requirements for installing and running a DB2 server are met. Otherwise, the End-to-End Automation Management component may not install or work properly.

DB2 server installation
You can use the DB2 Setup wizard to install the DB2 server. You find the DB2 Setup wizard on the CD labeled IBM DB2 Universal Database Enterprise Server Edition Version 9.1 for your platform.

The typical installation of a single-partition database environment is recommended.

On a Windows system, the following users must be local users:
• the DB2 administration server user
• the fenced user
• the instance owner user

You must create a DB2 instance before you install the End-to-End Automation Management component.

Make sure that the DB2 server has the required version level (see “Middleware software requirements” on page 81).

Make a note of the following information for future reference:
• The host name of the system where the DB2 server is installed.
• The port number of the DB2 instance
  The port number is displayed on the summary panel of the DB2 Setup wizard. The summary panel appears immediately before the wizard copies the program files.
• The name of the directory to which the DB2 server is installed if a local DB2 setup is used
• The name and password of the instance owner user or of a different user who is authorized to drop and create databases and database tables, and to select, insert, delete, and update table rows.

Post-installation tasks for remote DB2 setup

The following tasks must be completed on the DB2 server system:

- Identify the DB2 instance that will hold the databases. Identify the instance owner user ID and password. Identify the host name of the DB2 server system. Identify the TCP/IP port of the DB2 instance.
- Create the automation manager database (for information on how to do this, see below).
- Create the automation manager tables in the database (for information on how to do this, see below).

Note: If the database has already been created and tables already exist, you must drop the existing tables before creating the tables.

- To use a remote database setup, the following JDBC driver files must be copied from the remote database to a directory on the local system where the End-to-End Automation Management component will be installed:
  - db2jcc.jar
  - db2jcc_license_cu.jar

The CD IBM Tivoli System Automation Multiplatform V2.3.0 End-to-end component for your platform contains scripts for creating the required databases and tables.

Creating the automation manager database and the database tables:

On Windows: Perform the following steps if your DB2 server runs on a Windows system:

1. Log in with a user ID that has SYSADM privileges on the DB2 instance.
2. On the CD labeled IBM Tivoli System Automation Multiplatform V2.3.0 End-to-end component for Windows, change the directory to DDL\Script
3. From this directory, run the following batch file:
   
   `db2_create_automgr_db.bat <db_name> <instance_owner> <instance_pw>`

   where

   - `<db_name>` is the desired name of the automation manager database
     (Example: EAUTODB)
   - `<instance_owner>` is the instance owner user ID of the DB2 instance
     (Example: db2admin)
   - `<instance_pw>` is the password of the instance owner user ID

On AIX and Linux: Perform the following steps if your DB2 server runs under Linux or AIX:

1. Log in as root.
2. On the CD labeled IBM Tivoli System Automation Multiplatform V2.3.0 End-to-end component for your operating system, change the directory to DDL/Script.
3. From this directory, run the following shell script:

   `db2_create_automgr_db.sh <db_name> <instance_owner> <instance_pwd> <script_directory>`

   where

   - `<db_name>` is the desired name of the automation manager database
     (Example: EAUTODB)
   - `<instance_owner>` is the instance owner user ID of the DB2 instance
     (Example: db2inst1)
• <instance_pwd> is the password of the instance owner user ID
• <script_directory> directory where the DB2 scripts for Tivoli System Automation are located on the CD, which you changed to in step 2 (DDL/Script)

Verifying the creation of the remote database: After running the scripts as described in “Creating the automation manager database and the database tables” on page 86, issue the following commands to verify that the remote database was created correctly:
1. su - db2inst1
2. db2 connect to <db_name>
3. db2 list tables for schema eautosr
4. db2 disconnect <db_name>

The output of the list tables command should display the following table names:

<table>
<thead>
<tr>
<th>Table/View</th>
<th>Schema</th>
<th>Type</th>
<th>Creation time</th>
</tr>
</thead>
<tbody>
<tr>
<td>EEZAUTOMATIONACCESS EAUTOSR</td>
<td>2007-07-05-12.04.17.839700</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEZAUTOMATIONRELATION EAUTOSR</td>
<td>2007-07-05-12.04.18.379339</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEZDOMAINESSUBSCRIPTION EAUTOSR</td>
<td>2007-07-05-12.04.20.041327</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEZOOPERATORORDOMAINFILTER EAUTOSR</td>
<td>2007-07-05-12.04.18.970950</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEZOOPERATORHIDDENDOMAIN EAUTOSR</td>
<td>2007-07-05-12.04.20.060039</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEZRESOURCESUBSCRIPTION EAUTOSR</td>
<td>2007-07-05-12.04.20.513414</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Installing WebSphere Application Server

Before you begin:
• IBM Tivoli System Automation for Multiplatforms only supports the 32-bit version of WebSphere Application Server.
• WebSphere Application Server 6.1 Network Deployment is not supported.
• Installing WebSphere Application Server from the CD "IBM WebSphere Application Server Base Version 6.1" does not result in the required version level. To obtain the required version level 6.1.0.9, you must perform the following steps:
  1. Install WebSphere Application Server from the CD "IBM WebSphere Application Server Base Version 6.1."
  2. Install the WebSphere Application Server 6.1.0 UpdateInstaller.
  3. Use the UpdateInstaller to install the required fixes into WebSphere Application Server 6.1.
  4. Augment the application server of your WebSphere Application Server installation, or, preferably, augment every server profile into which you want to install the End-to-End Automation Management component.

These steps are described in the subsequent sections.

WebSphere Application Server 6.1.0.9 requirements

Check the following publication to find out which requirements need to be met for installing and running WebSphere Application Server Base:
• The ReadMe file, which is available on the product CD "IBM WebSphere Application Server Base Version 6.1".
• The "Getting started" topics in the Information Center for IBM WebSphere Application Server, Version 6.1.
• An IBM WebSphere Application Server Getting started document is also available on the product CD for your platform, where it is also referred to as Installation.
Guide. Make sure that all requirements for installing and running WebSphere Application Server are met. Otherwise, the End-to-End Automation Management component may not work properly.

The latest versions of all WebSphere Application Server publications can be found at

www.ibm.com/software/webservers/appserv/was/library/

In addition, check for the latest system requirements at

www.ibm.com/software/webservers/appserv/was/requirements/

Installing WebSphere Application Server 6.1.0.0

You can use the WebSphere Application Server installation wizard to install WebSphere Application Server. The WebSphere Application Server installation wizard can be started from the WebSphere Application Server LaunchPad. You find the LaunchPad on the CD labeled IBM WebSphere Application Server Version 6.1 for your platform.

The typical installation is recommended.

Upgrading WebSphere Application Server 6.1.0.0

Before you can install End-To-End Automation Management component of Tivoli System Automation for Multiprotocols 2.3, you must upgrade WebSphere Application Server 6.1.0.0 to level 6.1.0.9, upgrade the WebSphere Java version to Java 5 Service Release 5, and install the Advanced Edition of Integrated Solutions Console 7.1.

To do so, you use the WebSphere Application Server 6.1.0 upgrade CD for your platform (see “WebSphere Application Server upgrade CD” on page 76). The contents of the CD are listed in the following table.

To install the packages from the CD, you first install the UpdateInstaller (see “Installing the UpdateInstaller” on page 89) and use it to install the remaining packages (see “Installing Fix Pack 9, WASSDK, and the Advanced Edition of Integrated Solutions Console 7.1” on page 89).

Table 45. Contents of the WebSphere Application Server 6.1.0 upgrade CD

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contents</th>
</tr>
</thead>
</table>
| Fixes     | Three archives:  
• 6.1.0-WS-WAS-<your_platform>-FP0000009.pak  
Upgrades WebSphere Application Server 6.1.0.0 to level 6.1.0.9.  
• 6.1.0-WS-WASSDK-<your_platform>-FP0000009.pak  
Upgrades the Java version of WebSphere Application Server to Java 5, Service Release 5  
• 7.1.0.0-WS-WASFeature-FEISCAE7100.pak  
Installs the Advanced Edition of Integrated Solutions Console 7.1 |
| README    | The readme file README.txt. |
Table 45. Contents of the WebSphere Application Server 6.1.0 upgrade CD (continued)

<table>
<thead>
<tr>
<th>Directory</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade</td>
<td>The UpdateInstaller archive for your platform. You use the</td>
</tr>
</tbody>
</table>

Installing the UpdateInstaller: Perform these steps:
1. Unpack the appropriate zip file to a temporary directory. Unzipping creates the directories JDK and UpdateInstaller.
2. Change to the UpdateInstaller directory.
3. Invoke the file install to install the UpdateInstaller. When installed, the UpdateInstaller is located in the following directory by default:
   - AIX: /usr/IBM/WebSphere/UpdateInstaller/update.sh
   - Linux: /opt/IBM/WebSphere/UpdateInstaller/update.sh
   - Windows: C:\Program Files\IBM\WebSphere\UpdateInstaller\update.bat
4. Optional: Delete the temporary directory.

Installing Fix Pack 9, WASSDK, and the Advanced Edition of Integrated Solutions Console 7.1: You can install Fix Pack 9, WASSDK, and the Advanced Edition of Integrated Solutions Console 7.1 with one invocation of the UpdateInstaller. Fix Pack 9 should be the first package to be installed. WASSDK and Integrated Solutions Console can be installed in any sequence. If, for any reason, the UpdateInstaller does not install Fix Pack 9 first, remove the installed packages and install Fix Pack 9 first.

Augmenting the application server of your WebSphere Application Server installation: You need to augment the application server of your WebSphere Application Server installation, or, preferably, augment every server profile into which you want to install the End-to-End Automation Management component.

To do so, issue the following command (the example assumes that the profile name is AppSrv01 and the server name is server1):

```
<was_home>/bin/manageprofiles.sh
   -augment -templatePath <was_home>/profileTemplates/iscae71
   -profileName AppSrv01 -serverName server1
```

If the default path is used, `<was_home>` stands for:
- AIX: /usr/IBM/WebSphere/AppServer
- Linux: /opt/IBM/WebSphere/AppServer
- Windows: C:\Program Files\IBM\WebSphere\AppServer

Preparing for the installation of the End-to-End Automation Management component

Collecting the information you need to provide during installation

The installation of the End-to-End Automation Management component is wizard-driven. The wizard guides you through the installation and prompts you for installation and configuration parameters. The following tables list the parameters you need to specify on the installation wizard panels in the order in which they must be specified.
Make sure that you specify all required parameters on the installation wizard panels and that your entries are correct. The installation wizard does not verify that your entries are correct and complete during the installation.

**Installation directory and Tivoli Common Directory**

The parameters listed in the following table must always be specified.

*Table 46. Installation directory and Tivoli Common Directory*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation directory name</td>
<td>The directory to which the installable features are installed.</td>
<td>Windows: C:\Program Files\IBM\tsamp\eez</td>
</tr>
<tr>
<td></td>
<td>In this guide, this directory is referred to as EEZ_INSTALL_ROOT.</td>
<td>AIX, Linux: /opt/IBM/tsamp/eez</td>
</tr>
<tr>
<td></td>
<td>When specifying a directory other than the default, observe the following restrictions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Windows:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The colon character is allowed only once, immediately following the drive letter. For example, C:&lt;directory_name&gt; is allowed, but C:&lt;directory_name&gt;:&lt;directory_name&gt; is not allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The space character and the underscore character (_) are allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AIX, Linux:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The underscore character (_) is allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The space and colon characters are not allowed.</td>
<td></td>
</tr>
</tbody>
</table>
Table 46. Installation directory and Tivoli Common Directory (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Common Directory</td>
<td>The Tivoli directory for storing serviceability information.</td>
<td>Windows:</td>
</tr>
<tr>
<td></td>
<td>During installation, you are only prompted for input when no Tivoli Common</td>
<td>C:\Program Files\IBM\tivoli\common</td>
</tr>
<tr>
<td></td>
<td>Directory is found on the system.</td>
<td>AIX, Linux:</td>
</tr>
<tr>
<td></td>
<td>In the Tivoli Common Directory, the subdirectory eez is created for storing</td>
<td>/var.ibm/tivoli/common</td>
</tr>
<tr>
<td></td>
<td>product-specific data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this guide, this directory is referred to as Tivoli_Common_Directory.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When specifying a directory other than the default, observe the following</td>
<td></td>
</tr>
<tr>
<td></td>
<td>restrictions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Windows:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The directory name has to consist of the platform-specific path separator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>character and alphanumeric characters (A..Z, a..z, 0..9).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The colon character is allowed only once, immediately following the drive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>letter. For example, C:&lt;directory_name&gt; is allowed, but</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C:&lt;directory_name&gt;:&lt;directory_name&gt; is not allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The space character and the underscore character (_) are allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>AIX, Linux:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The directory name has to consist of the platform-specific path separator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>character and alphanumeric characters (A..Z, a..z, 0..9).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The underscore character (_) is allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The space and colon characters are not allowed.</td>
<td></td>
</tr>
</tbody>
</table>

### Installation parameters for DB2

**Note:** When you have a local DB2 setup but do not want the installation wizard to create the end-to-end automation management database and the database tables, just select the radio button for remote DB2 setup (**IBM DB2 UDB on different system (remote)**) on the Database Server window of the installation wizard. If you make this selection, the installation wizard will neither create the database nor any tables and you are free to set up the database manually as you would for remote setup.

The parameters listed in the following table must be specified.
### Table 47. DB2 data for local and remote DB2 setup

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2 UDB directory</td>
<td>The installation location of the DB2 client directory. If you are using a local DB2 setup, you use the DB2 client that is part of the DB2 server installation. In this case, you need to specify the DB2 server directory.</td>
<td>The location is detected on your system and displayed as default directory.</td>
</tr>
<tr>
<td>DB2 instance host name</td>
<td><strong>Remote DB2 setup:</strong> The host name of the DB2 instance in which the automation manager and operations console databases are located.</td>
<td></td>
</tr>
<tr>
<td>DB2 instance port number</td>
<td>The port number of the DB2 instance in which the automation manager and operations console databases are located. <strong>Note:</strong> When you install the End-to-End Automation Management component on AIX or Linux systems, the installation wizard can retrieve the valid DB2 instance port number automatically. If you opt not to use this function, or on Windows systems, the port number 50000 will be displayed in the entry field on the corresponding installation wizard panel, which is the default port number that is assigned to DB2 during the installation of DB2. However, if the port is not free, a different port number is assigned automatically, which is why you need to check if the default port number is correct. How you determine the correct port number is described in &quot;Determining the correct DB2 port number&quot; on page 243.</td>
<td>50000</td>
</tr>
<tr>
<td>Database instance owner name</td>
<td>The instance owner user ID of the DB2 instance in which the automation manager and operations console databases are located.</td>
<td>Windows: db2admin&lt;br&gt; AIX, Linux: db2inst1</td>
</tr>
<tr>
<td></td>
<td>In a local DB2 setup, this user ID will be used for creating the databases and tables.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In a remote DB2 setup, the database and the tables must have already been created. The installation program does no change to DB2 and neither creates a DB nor tables.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The user ID will be used by WebSphere Application Server to connect to the automation manager and operations console databases and to select, insert, delete, and update rows in tables.</td>
<td></td>
</tr>
</tbody>
</table>
Table 47. DB2 data for local and remote DB2 setup (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database instance owner password</td>
<td>The password for the instance owner user ID of the DB2 instance in which the automation manager and operations console databases are located.</td>
<td>No default value is provided</td>
</tr>
<tr>
<td>DB2 UDB JDBC driver path on local system</td>
<td>For remote DB2 setup only: Path to the directory where the files DB2 JDBC are located.</td>
<td>EAUTOJDB</td>
</tr>
<tr>
<td>Automation manager database</td>
<td>Automation manager database for use by WebSphere Application Server. In a local DB2 setup, a database with this name will be created in the DB2 instance related to the specified instance owner. In a remote DB2 setup, a database with this name must already exist in the remote DB2 instance.</td>
<td>EAUTOJDB</td>
</tr>
</tbody>
</table>

WebSphere Application Server installation parameters
The parameters listed in the following table are detected during the installation of the End-to-End Automation Management component.

Note that WebSphere Application Server security must be enabled before you install the End-to-End Automation Management component.

Table 48. WebSphere Application Server installation parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSphere Application Server directory</td>
<td>The installation location of WebSphere Application Server. There must be exactly one installation of WebSphere Application Server on your system.</td>
<td>The location is detected on your system and displayed as default directory.</td>
</tr>
<tr>
<td>WebSphere Application Server (WAS) profile name</td>
<td>The WebSphere Application Server profile to be used for the automation manager and the operations console.</td>
<td>All existing profiles are detected on your system and displayed in a single-choice list.</td>
</tr>
<tr>
<td>WebSphere Application Server (WAS) server name</td>
<td>The server to be used for the automation manager.</td>
<td>The server name is detected on your system and displayed as default value.</td>
</tr>
<tr>
<td>WAS Admin User ID</td>
<td>The user ID of the WebSphere Application Server administrator.</td>
<td>No default value is provided.</td>
</tr>
<tr>
<td>WAS Admin User Password</td>
<td>The password of WebSphere Application Server administrator user ID.</td>
<td>No default value is provided.</td>
</tr>
</tbody>
</table>
IBM Tivoli Enterprise Console connection configuration data
Optionally, you can use Tivoli Enterprise Console for monitoring end-to-end
automation management events. The parameters listed in the following table are
only required if you will be utilizing Tivoli Enterprise Console for end-to-end
automation management.

Table 49. Installation parameters for IBM Tivoli Enterprise Console

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEC host name</td>
<td>The name of the host where the Tivoli Enterprise Console server is installed.</td>
<td>localhost</td>
</tr>
<tr>
<td>TEC server port number</td>
<td>The port number for the Tivoli Enterprise Console server</td>
<td>5529</td>
</tr>
</tbody>
</table>

For more information about utilizing Tivoli Enterprise Console for end-to-end
automation management, refer to the IBM Tivoli System Automation for
Multiplatforms End-to-End Automation Management Component Administrator’s and

Name of the end-to-end automation domain

Table 50. Name of the end-to-end automation domain

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation domain name</td>
<td>The name of the end-to-end automation domain represented by this instance of the automation engine. The domain name must be unique and may not be used for any other automation domain. The characters used for the domain name are limited to the following ASCII characters: A-Z, a–z, 0-9, . (period), and _(underscore)</td>
<td>FriendlyE2E</td>
</tr>
</tbody>
</table>

WebSphere Application Server user ID for the end-to-end
automation engine
The end-to-end automation engine requires a WebSphere Application Server user
ID to access the J2EE framework. The user ID is created during the installation of
the End-to-End Automation Management component. In the installation wizard,
you need to specify the user ID and the password.

Table 51. Name of the end-to-end automation domain

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>WebSphere Application Server user ID for the end-to-end automation engine</td>
<td>eezdmn</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the user ID</td>
<td></td>
</tr>
</tbody>
</table>

System Automation Administrator User ID
During the installation of the End-to-End Automation Management component, the
initial Tivoli System Automation administrator user is created in WebSphere
Application Server and authorized for all tasks and actions that can be performed
from the SA operations console. In the installation wizard, you need to specify the
data listed in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>User ID of the SA operations console administrator</td>
<td>eezadmin</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the user ID</td>
<td>none</td>
</tr>
<tr>
<td>First and last name of the user</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

**What the installation CD contains**

The End-to-End Automation Management component can be ordered from IBM as media pack or downloaded as an Electronic Software Distribution (ESD) image from an IBM software distribution download site.

There are multiple CDs for each supported platform.

This is what the CD labeled *IBM Tivoli System Automation Multiplatform V2.3.0 End-to-end component for <operating_system_name>* contains:

- The files for launching the installation wizard
- The readme file
- Directories containing the files required to install components that are embedded into the end-to-end automation management installation. These are:

  **Table 52. Directories on the product CD**

<table>
<thead>
<tr>
<th>Directory</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>README</td>
<td>For example, copyright notices and license agreements</td>
</tr>
<tr>
<td>license</td>
<td>License key</td>
</tr>
<tr>
<td>DDL</td>
<td>Scripts for creating DB2 databases and tables when remote DB2 setup is used</td>
</tr>
<tr>
<td>&lt;PLATFORM&gt;¹</td>
<td>Product installer and files needed for installing the product</td>
</tr>
</tbody>
</table>

**Note:**

1. <PLATFORM> is one of the following:
   * AIX
   * PPC (Linux on POWER)
   * Windows
   * i386 (Linux on System x)
   * S390 (Linux on System z)

**Languages and locales supported by the End-to-End Automation Management component**

If you want to use the End-to-End Automation Management component in a language other than English, or if your default system locale is a non-English locale, use the following sections to find out which languages and locales are supported.

**Languages supported on Linux systems**

[Table 53 on page 96] shows the combinations of languages and locales that are supported by the End-to-End Automation Management component on Linux systems to display messages. When you are using the end-to-end automation adapter of the Base component, note that UTF-8 encoding is always supported, but new versions of Linux operating systems may not support all of the listed languages.
Table 53. Languages and locales supported by End-to-End Automation Management component on Linux systems

<table>
<thead>
<tr>
<th>Language</th>
<th>UTF-8</th>
<th>ISO-8859-1</th>
<th>EUC/GBK</th>
<th>Euro</th>
<th>GB18030/BIG5</th>
</tr>
</thead>
<tbody>
<tr>
<td>German</td>
<td>de_DE.UTF-8</td>
<td>de_DE, de_DE.ISO-8859-1</td>
<td>de_DE@euro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>es_ES.UTF-8</td>
<td>es_ES, es_ES.ISO-8859-1</td>
<td>es_ES@euro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>French</td>
<td>fr_FR.UTF-8</td>
<td>fr_FR, fr_FR.ISO-8859-1</td>
<td>fr_FR@euro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italian</td>
<td>it_IT.UTF-8</td>
<td>it_IT, it_IT.ISO-8859-1</td>
<td>it_IT@euro</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japanese</td>
<td>ja_JP.UTF-8</td>
<td>ja_JP.eucJP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Korean</td>
<td>ko_KR.UTF-8</td>
<td>ko_KR.eucKR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazilian Portuguese</td>
<td>pt_BR.UTF-8</td>
<td>pt_BR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>zh_CN.UTF-8</td>
<td>zh_CN, zh_CN.GBK, zh_CN.GB18030</td>
<td>zh_TW, Big5, zh_TW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traditional Chinese</td>
<td>zh_TW.UTF-8</td>
<td>zh_TW</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Languages and locales supported on AIX systems

The table below lists the combinations of languages and locales that are supported by the End-to-End Automation Management component on AIX systems to display messages.

Table 54. Languages and locales supported by the End-to-End Automation Management component on AIX systems

<table>
<thead>
<tr>
<th>Language</th>
<th>UTF-8</th>
<th>ISO-8859-1</th>
<th>EUC/GBK</th>
<th>SJIS/GB18030/BIG5</th>
</tr>
</thead>
<tbody>
<tr>
<td>German</td>
<td>DE_DE</td>
<td>de_DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanish</td>
<td>ES_ES</td>
<td>es_ES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>French</td>
<td>FR_FR</td>
<td>fr_FR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Italian</td>
<td>IT_IT</td>
<td>it_IT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Korean</td>
<td>KO_KR</td>
<td>ko_KR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brazilian Portuguese</td>
<td>PT_BR</td>
<td>PT_BR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>ZH_CN</td>
<td>zh_CN</td>
<td>ZH_CN</td>
<td></td>
</tr>
<tr>
<td>Traditional Chinese</td>
<td>ZH_TW</td>
<td>zh_TW</td>
<td>ZH_TW</td>
<td></td>
</tr>
</tbody>
</table>

Installation prerequisites

The following prerequisites must be satisfied before you can start the installation wizard for the End-to-End Automation Management component:

- The 32-bit version of WebSphere Application Server must be installed as described in "Installing WebSphere Application Server" on page 87. No other WebSphere Application Server product installation must exist on the system.
- A DB2 server must be installed as described in "Installing a DB2 server" on page 84. The DB2 server instance must be running and accepting client connections.

For more information on setting up the DB2 environment, refer to Chapter 1.

"Before creating a database" -> "Preparing to create a database" in IBM DB2 Universal Database Administration Guide: Implementation, Version 9.1 (SC09-4820).
• If an automation manager database (EAUTODB) from an earlier installation already exists, for example, if you are upgrading from IBM Tivoli System Automation 2.2 to 2.3, in which case you need to uninstall the older version before installing the new, the database will be dropped without warning during the installation of the End-to-End Automation Management component. To preserve the data from the earlier installation, you can export the data before starting the uninstallation, and import it during the installation. For information on exporting the data before uninstalling, see Appendix A, “Preserving user data during the upgrade from IBM Tivoli System Automation 2.2 to IBM Tivoli System Automation 2.3,” on page 235.

• In the current RedHat 5 distributions, the SElinux environment is switched on by default. It must be switched off for IBM Tivoli System Automation to work properly.

• The user ID that is used to run the installer for the End-to-End Automation Management component must have administrator authority.

  On Linux and AIX, this user ID is typically “root”.

• When installing the End-to-End Automation Management component to an AIX or Linux system, you must ensure that an XWindows session is available for displaying the graphical installation wizard panels.

### Installing the End-to-End Automation Management component using the installation wizard

This section describes how to install the End-to-End Automation Management component. For the installation, you use a graphical installation program, the so-called installation wizard. The required steps are described below.

On the panels of the installation wizard, enter the data you have collected using the lists in section “Collecting the information you need to provide during installation” on page 89. Make sure that you specify all required parameters on the installation wizard panels and that your entries are correct. The installation wizard does not verify that you entries are correct and complete during the installation.

**Notes:**

1. The installation wizard panels in this section show an installation on an AIX system. The wizard panels that are displayed during the installation on other operating systems are very similar. Make sure to conform to the conventions of your platform when specifying directory locations, files names and so on.

2. In this section, only those panels are depicted on which user actions are required.

3. The installation comprises these phases:
   a. In the pre-installation phase, you specify the installation parameters. This may take up to an hour.
   b. The installation phase, which begins when you click the Install button on the last pre-installation panel. In this phase, all files are installed to the disk.
   c. The configuration step, in which the necessary WebSphere Application Server and DB2 configuration is performed. The configuration step can be canceled at any time. The installation can be resumed by simply calling the installer again.

To install the End-to-End Automation Management component, perform these steps:
1. Make sure that all installation prerequisites are met (refer to "Installation prerequisites" on page 96).

2. Insert the following CD into the CD drive:
   IBM Tivoli System Automation Multiplatform V2.3.0 End-to-end component for <operating_system_name>
   There are multiple CDs. Be sure to use the one for your platform.

3. Change to the directory that contains the installation program. For the location of the directory, refer to "Packaging" on page 75.

4. Launch the installation wizard by starting the following program from the current working directory:
   - **Windows**: setup.exe
     To generate a response file for use in a silent installation, use the following command to launch the wizard:
     ```shell
     setup.exe -Dpreparesilent=true
     ```
   - **AIX, Linux**: setup.bin
     To generate a response file for use in a silent installation, use the following command to launch the wizard:
     ```shell
     setup.bin -Dpreparesilent=true
     ```

When the installation wizard is ready, the initial wizard window appears:
5. Select the language in which the text on the wizard panels is to appear and click OK. The language in which the End-to-End Automation Management component is installed is derived from the system’s locale setting.

6. Read the information on the Introduction panel and click Next.

7. Carefully read the terms of the license agreement. Make sure to also read the non-IBM terms by clicking Read non-IBM terms.

   To accept the terms of the license agreement, select I accept both the IBM and the non-IBM terms and click Next.

9. Specify the directory where you want to install the End-to-End Automation Management component or accept the default location.
   Click Next.

10. If the installation program detected a Tivoli Common Directory on your system, for example, because a Tivoli product is already installed, the directory must also be used for IBM Tivoli System Automation for Multiplatforms. In this case, the entry field on the panel is write-protected.
    If the installation program did not detect a Tivoli Common Directory on your system, accept the default location or specify the directory to which the Tivoli log files are to be written.
    Click Next.
11. Select the DB2 setup type you are using and click Next.

Which panel appears next, depends on the type of DB2 setup you selected:
- **Local DB2 setup**: Proceed with step 12
- **Remote DB2 setup**: Proceed with step 15 on page 103

12. **This panel only appears when you are using a local DB2 setup.**
Specify the database name or accept the default name and click Next. Note that an existing EAUTODB will be dropped automatically without warning (for information on preserving existing data, see Appendix A, “Preserving user data during the upgrade from IBM Tivoli System Automation 2.2 to IBM Tivoli System Automation 2.3,” on page 235).
13. This panel only appears when you are using a local DB2 setup. Specify the name and password of the DB2 instance owner and click Next.

14. This panel only appears when you are using a local DB2 setup. In the field **DB2 instance port number**, the valid port number must be specified:
   - If the DB2 port number was retrieved automatically, the valid port number is displayed in the field.
   - If the DB2 port number was not retrieved automatically, the default port number (50000) is displayed. The actual DB2 port number may differ from the default, because a different port number is assigned automatically during DB2 installation if the default port is not free. Before you accept the default value, ensure that it is correct, or specify the valid port number. Click **Next** and proceed with step 18 on page 105.
Note: After you click Next, the installation program checks whether the database can be accessed with the values you specified on the panel. If you want to skip the check, select the check box on the panel.

15. This panel only appears when you are using a remote DB2 setup. Specify the database name (see “Post-installation tasks for remote DB2 setup” on page 86), and click Next.

16. This panel only appears when you are using a remote DB2 setup. Specify the path to the DB2 UDB JDBC driver or click Choose to select the directory (see “Post-installation tasks for remote DB2 setup” on page 86), and specify the name and password of the database instance owner. Click Next.
17. This panel only appears when you are using a remote DB2 setup.

In the field **DB2 server host name**, specify the fully qualified host name of the system where the DB2 server is installed.

In the field **DB2 server port**, the valid port number must be specified:

- If the DB2 port number was retrieved automatically, the valid port number is displayed in the field.

- If the DB2 port number was not retrieved automatically, the default port number (50000) is displayed. The actual DB2 port number may differ from the default, because a different port number is assigned automatically during DB2 installation if the default port is not free. Before you accept the default value, ensure that it is correct, or specify the valid port number.

**Note:** After you click **Next**, the installation program checks whether DB2 can be accessed with the values you specified on the panel. If you want to skip the check, select the check box on the panel.
18. If you want to import existing data into the new end-to-end automation database, select the Import data check box and specify the fully qualified directory name in which the exported data is located.

For information on how to export data from an existing end-to-end automation database in such a way that it is ready for import, see Appendix A, “Preserving user data during the upgrade from IBM Tivoli System Automation 2.2 to IBM Tivoli System Automation 2.3,” on page 235.

19. The installation directory of WebSphere Application Server is detected on your system and displayed. Click Next.
20. The existing WebSphere Application Server profiles are detected on your system and displayed. Select the profile you want to use and click Next.

21. Specify the end-to-end automation domain name you want to use or accept the default name and click Next.

Note: Accept the default domain name ("FriendlyE2E") if you want to use the sample end-to-end automation management environment to familiarize yourself with end-to-end automation management and the operations console. For more information, refer to the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide section “Getting started.”
22. If you want to use Tivoli Enterprise Console to display end-to-end automation management events:

- Select **Enable TEC server connection**
- In the field **TEC host name**, specify the host name of the console server.
- In the field **TEC server port number**, specify the port number of the console server:
  - **Windows**: Accept the default value that is displayed in the field (5529)
  - **AIX/Linux**: Set the value to 0

Click **Next**.

**Note:** You can also enable the connection from the WebSphere Application Server administrative console after the installation of the End-to-End Automation Management component is complete. This is described in the [IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide](https://www.ibm.com/support/knowledgecenter/SSEK79_6.3.0/com.ibm.etools.ntadm.doc/aem/ua sett.html) in section “Using Tivoli Enterprise Console with SA for Multiplatforms”.
23. Specify the WebSphere Application Server user ID and password for the end-to-end automation engine. The automation engine will use the credentials for accessing the J2EE framework that runs in WebSphere Application Server.

24. Specify the user ID, password, and the first and last name of the System Automation administrator. Do not use cut-and-paste to enter the password and the password confirmation, rather, directly type in the password and the password confirmation.
   Click Next.
25. When you have specified all the required information on the wizard panels, a summary panel appears. As the installation wizard will not check the available space, be sure to verify that sufficient space is available in the file system.

Click **Install** to start the installation. The installation can take considerable time to complete.

26. While the component is being installed and configured, a number of information panels inform you of the progress.
27. When the installation of the End-to-End Automation Management component is complete, the Installation Complete panel appears. Click **Done** to close the installation wizard. For information on verifying the installation, refer to “Verifying the installation” on page 111.

---

**Installing the End-to-End Automation Management component in silent mode**

You can install the End-to-End Automation Management component in silent mode, using a response file you generated in a wizard-driven installation (see “Installing the End-to-End Automation Management component using the installation wizard” on page 97.)
After the wizard-driven installation is complete, you find the response file
install.properties in the following directory:
<EEZ_INSTALL_ROOT>/install

Note that this files is always generated, even if you did not specify the option
-Dpreparesilent=true when you invoked the installation wizard. However, install.properties files created without the -Dpreparesilent=true option cannot
be used for silent installation.

To perform a silent installation, perform these steps:
1. Copy the response file install.properties file to the system on which you
   want to perform the silent installation.
2. To start the installation, issue this command:
   
   **Windows:**
   
   ```
   setup.exe -i silent -f <fully_qualified_properties_file_name>
   ```
   
   **AIX, Linux:**
   
   ```
   setup.bin -i silent -f <fully_qualified_properties_file_name>
   ```

---

**Verifying the installation**

**Automation manager**

To verify that the automation manager was installed successfully, complete the
tasks described in the following sections.

**End-to-end automation database**

Perform these steps to verify that the end-to-end automation database and the
database tables were created successfully:
1. Ensure that DB2 is running.
2. Open the DB2 Control Center.
3. Navigate to Databases and expand the folder.
4. Expand EAUTODB.
5. Click Tables. The following database tables must be listed:
   - EEAUTOMATIONACCESS
   - EEAUTOMATIONRELATION
   - EEZDOMAINESSUBSCRIPTION
   - EEZOPERATORDOMAINFILTER
   - EEZOPERATORDOMAINPREFERENCES
   - EEZOPERATORHIDDENDOMAIN
   - EEZRESOURCESUBSCRIPTION

**Automation J2EE Framework**

Perform these steps to verify that the automation J2EE framework was installed
successfully:
1. In a Web browser window, specify the following address to display the Login
   panel of Integrated Solutions Console:
   ```
   http://<your_host_name>:<your_isc_port>/ibm/console
   ```
   
   The default port is 9060.
2. On the login panel, enter the user ID and password of the WebSphere
   Application Server administrator user.
3. Navigate to Applications > Enterprise Applications. The list of installed applications must contain the entry EEZEAR.

**Verifying that DB2 accepts WebSphere Application Server requests**

Perform the following task to verify that DB2 accepts WebSphere Application Server requests:

1. In a Web browser window, specify the following address to display the Login panel of Integrated Solutions Console:
   
   \[ \text{http://<your_host_name>:<your_isc_port>/ibm/console} \]

   The default port is 9060.

2. On the login panel, enter the user ID and password of the WebSphere Application Server administrator user.

3. Navigate to Resources > JDBC > Data sources > EAUTODBDS. Click Test connection to verify that DB2 accepts WebSphere Application Server requests. If the test is successful, the following message comes up:
   
   Test connection for data source EAUTODBDS was successful.

   If the test fails, check if the DB2 port number specified for EAUTODB is correct (for more information, refer to the "Troubleshooting" appendix in the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide section “WebSphere Application Server cannot connect to DB2”.

**Automation engine**

Perform these steps to verify that the automation engine was installed successfully:

1. Issue the command `ezzdmn -?`. When the installation of the automation engine was successful, the list of available command options is displayed.

   **Note:** You can also use any of the other `ezzdmn` command options to verify the installation of the automation engine. As long as you do not receive an exception, any message you receive verifies that the automation engine is installed correctly. For a complete list of the `ezzdmn` command options, refer to the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide chapter “Using the command-line interface of the automation engine”.

**Operations console**

Perform the following steps to verify that the operations console was installed successfully:

1. In a Web browser window, specify the following address to display the Login panel of Integrated Solutions Console:
   
   \[ \text{http://<your_host_name>:<your_isc_port>/ibm/console} \]

   The default port is 9060.

2. On the Log in panel of Integrated Solutions Console, enter the System Automation administrator user ID. The default user ID is eezadmin. Click Log in.
3. On the Welcome page of Integrated Solutions Console, click the entry for Tivoli System Automation for Multiplatforms.

Figure 5. Log in panel of Integrated Solutions Console

Figure 6. Welcome panel of Integrated Solutions Console
4. When the Welcome page of Tivoli System Automation for Multiplatforms is displayed, the installation was successful.

Post-installation tasks

When you have verified the installation of the End-to-End Automation Management component, you need to perform a number of post-installation tasks:

- You must create and authorize additional users as described in the [IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide](#).
- You must enable the end-to-end automation manager to access the first-level automation domains.

To do this, you must specify the user credentials for the first-level domains on the User credentials tab of the configuration dialog.

“Invoking the end-to-end automation manager configuration dialog” on page [119](#) describes how you launch the configuration dialog. For detailed information about the User credentials tab, refer to the online help of the configuration dialog.

- To get end-to-end automation management operational, you must create and activate an automation policy. This is described in the [IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide](#).

Modifying the LTPA settings

After the installation of the End-to-End Automation Management component, you should check whether the LTPA settings are appropriate for your environment.

During installation, the following LTPA parameters are automatically set in WebSphere Application Server:

- LTPA Password is set to the password of the Integrated Solutions Console administrator user ID
- LTPA Timeout is set to 120 minutes

LTPA Timeout is a security-related timeout. Because this timeout is absolute, a user will be logged out and forced to log in to Integrated Solutions Console again when the LTPA timeout is reached even if the user is working with the operations console at the time.

To change the LTPA settings (for example, password and timeout) you use the WebSphere Application Server administrative console. On the administrative console, select Security > Secure administration, applications, and infrastructure > Authentication mechanisms and expiration.

Modifying the HTTP session timeout

After the installation of the End-to-End Automation Management component, you should check whether the setting of the HTTP session timeout is appropriate for your environment.

The HTTP session time is an activity timeout. The value to which the HTTP session timeout is set defines after how many minutes of inactivity a user is logged out automatically.

During installation, the HTTP session timeout is set to 30 minutes.
To change the value, you use the WebSphere Application Server administrative console.

On the administrative console, select **Servers > Application servers > server1 > Container Settings > Session Management**:

![Integrated Solutions Console](image)

**Configuring how many users can connect to the automation manager using the operations console**

During the installation of the End-to-End Automation Management component, a default value is set that defines how many users can simultaneously connect to the automation manager using the SA operations console. You can change the current setting by changing the **Maximum connections** value for the EEZTopicConnectionFactory from Integrated Solutions Console (**Resources > JMS > Topic connection factories > EEZTopicConnectionFactory > Connection pools**).

If **Maximum connections** is set to 0, the number of concurrent connections that can be established is allowed to grow infinitely. If the specified number of maximum connections is reached, the next connection attempt using the operation console will bring up the following error message:

**EEZU0011E:**
Unable to set up the event path between the operations console and the management server:
**CWSIAD005E:** The JCA runtime failed to allocate a connection.

---

Chapter 10. Installing the End-to-End Automation Management component 115
Chapter 11. Upgrading the End-to-End Automation Management component from release 2.2

To upgrade from release 2.2 of the End-to-End Automation Management component to release 2.3, the release 2.2 must be uninstalled and release 2.3 must be installed.

To preserve the data from the earlier installation, you can export the data before starting the uninstallation, and import it during the installation of release 2.3. For information on exporting the data before uninstalling, see Appendix A, “Preserving user data during the upgrade from IBM Tivoli System Automation 2.2 to IBM Tivoli System Automation 2.3,” on page 235.
Chapter 12. Configuring the end-to-end automation manager

This chapter provides an overview of how you use the end-to-end automation manager configuration dialog to perform the following tasks:

- Change the basic configuration of the end-to-end automation manager (see “End-to-end automation manager basic configuration” on page 121).
- Configure high availability for the end-to-end automation manager (see “Configuring high availability for the end-to-end automation manager” on page 128).

Invoking the end-to-end automation manager configuration dialog

Before you begin:

The user ID you use to invoke the dialog must meet the following requirements:

- The user ID must be in same group as the user ID you used for installing the End-to-End Automation Management component. The group permissions for cfgeezdmn.sh must be set to EXECUTE.
- The user ID must have read-write permissions on the following directory:
  - Windows: <EEZ_INSTALL_ROOT>/cfg
  - AIX and Linux:/etc/<EEZ_INSTALL_ROOT>/cfg

Make sure that the bits are set correctly.

Perform the following step to invoke the configuration dialog:
1. Log in on the system where the End-to-End Automation Management component is installed.

2. Enter the following command:
   - Windows: cfgeezdmn.bat
   - AIX and Linux: cfgeezdmn

   The configuration dialog task launcher is displayed (see Figure 7 on page 120).

Using the task launcher

The task launcher appears when you invoke the configuration dialog as described in “Invoking the end-to-end automation manager configuration dialog.”
Click **Configure** to open the end-to-end automation manager configuration dialog. On the dialog tabs, you specify basic configuration parameters. For more information, see “End-to-end automation manager basic configuration” on page 121.

### High-availability configuration

You perform the tasks in this section to provide high availability for your end-to-end automation manager. You activate the task buttons by selecting **Enable the high availability configuration tasks**.

Note that on Windows operating systems, high-availability configuration is not supported and all tasks are disabled. For more information, see “Configuring high availability for the end-to-end automation manager” on page 128.

**Displaying online help**

The following sections provide an overview of the end-to-end automation manager configuration tasks. More detailed information is available in the online help. To launch the online help, click **Help** on a dialog tab:
End-to-end automation manager basic configuration

The initial configuration of the end-to-end automation manager is performed during the installation of the End-to-End Automation Management component. To browse or change the properties, you always use the end-to-end automation manager configuration dialog. You never manually edit the configuration properties files in which the configuration parameters are stored.

The following sections describe the basic configuration tabs of the end-to-end automation manager configuration dialog. To open the configuration dialog, perform these steps:

1. Invoke the configuration dialog (see “Invoking the end-to-end automation manager configuration dialog” on page 119).
2. On the task launcher, click Configure in the "End-to-end automation manager basic configuration" area. The basic configuration notebook appears (see Figure 8 on page 122). The tabs of the notebook are described in the following sections.

Post-configuration tasks:

After changing any of the configuration properties, you must perform the following tasks:

- Activate the new settings by reconfiguring the automation engine. To do so, invoke the command eeZDMN with the option -reconf.
  For command details, see the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide section "Using the command-line interface of the automation engine".

- If your end-to-end automation manager is configured for high availability, you must replicate the configuration files to the other nodes of the Base component domain that provides the high availability.
Note: For a change in the policy pool location on the Domain tab to become effective, the automation engine must be restarted using `eezdmn -shutdown` and `eezdmn -start`.

**Domain tab**

Use the tab to browse or change the configuration properties of the end-to-end automation domain.

![Domain tab configuration](image)

*Figure 8. Domain tab*

**Fields on the Domain tab:**

**Domain name**

The name of the end-to-end automation domain. The name in this field must be specify in the XML element `<AutomationDomainName>` in each of the domain's automation policy files. Only the following ASCII characters can be used for the domain name: A-Z, a–z, 0-9, . (period), and _ (underscore).

**Host name or IP address**

Name or IP address of the system that hosts the end-to-end automation manager.

**WAS bootstrap port number**

The bootstrap port of the WebSphere Application Server instance that hosts the end-to-end automation manager.

**Command line request port number**

The port on which the automation engine receives command-line interface requests.

**Event port number**

The port on which the EIF message converter listens for events from the first-level automation domains. The port number specified here must
match the port number specified as event port number for the end-to-end automation management host when configuring automation adapters on first-level automation domains.

For SA for z/OS, this is the event port specified in the adapter configuration parameter eif-send-to-port in the adapter plug-in properties file.

**Policy pool**

The fully qualified name of the directory that contains the XML automation policy files for the end-to-end automation domain. Only automation policy files that are available in this directory can be activated.

*Note:* For a change in the policy pool location to become effective, the automation engine must be restarted using `ezdnn -shutdown` and `ezdnn -start`.

**Command shell tab**

The end-to-end automation manager requires authentication when a user invokes the end-to-end automation manager command shell. By default, users are always prompted for their user credentials. On the Command shell tab you have the choice between these authentication modes:

**Read user credentials from stdin**

In this mode, users must always specify their user credentials in the shell window.

**Prompt for user authentication**

In this mode, users are always prompted for their credentials unless they specify them when they invoke the command shell.

**Use specified user credentials**

In this mode, a shared user ID is used for authentication, which prevents users from being prompted for their credentials when they invoke the command shell.
You specify the shared user ID and the corresponding password in the fields **User ID** and **Password**. Note that only the following ASCII characters can be used for the user ID: A-Z, a–z, 0-9, and _ (underscore).

To change the password, click **Change**.

**User credentials tab**

Use the tab to browse or change the user credentials of the end-to-end automation manager. The automation manager uses these credentials to authenticate itself. The characters used for all credentials entered on this tab are limited to the following ASCII characters: A-Z, a–z, 0-9, and _ (underscore).

![End-to-End Automation Manager Configuration](image)

Fields on the User credentials tab:

**WAS access user ID**

The user ID that is used to access the WebSphere Application Server instance that hosts the end-to-end automation manager.

**WAS access user password**

The password for the WAS access user ID. Click **Change** to change the password.

**Generic user ID**

The user ID the automation manager uses to authenticate itself to a first-level automation domain when no credentials are specified for the domain in **Credentials for accessing specific first-level automation domains**.

**Generic password**

The password for the generic user ID. Click **Change** to change the password.

**Credentials for accessing specific first-level automation domains**

Click **Add** to specify a user ID that is valid for the domain. The user ID
need not be root but it should be authorized to perform operations on resources in the first-level automation domain that the end-to-end automation manager supports, for example, bringing an automated resource online. The Remove and Change buttons let you create and modify the credentials for a first-level automation domain.

Security tab

Use the tab to browse and change the configuration properties for the SSL connection to the first-level automation domains.

Fields on the Security tab:

Truststore
The fully qualified file name of the truststore file that is used for SSL. The truststore path name must follow the same naming rules as the Installation Directory Name (see Table 46 on page 90). The file name may contain multiple period characters. Click Browse to select a file.

Keystore
The fully qualified file name of the keystore file that is used for SSL. The keystore path name must follow the same naming rules as the Installation Directory Name (see Table 46 on page 90). The file name may contain multiple period characters. Click Browse to select a file.

Keystore password
The password of the keystore file. The password is required if a keystore file was specified. Click Change to change the password.

Note: If the truststore is in different file than keystore, the passwords for the files must be identical.
Certificate alias
The alias name of the certificate to be used by the server. The characters used for the certificate alias are limited to the following ASCII characters: A-Z, a-z, 0-9, and _ (underscore)

Logger tab
Use the tab to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the properties file.

On the Logger tab, you can perform the following tasks:

Change the settings permanently
Perform these steps:
1. Make the required changes on the tab.
2. Click Save.

Results:
The settings in the properties file are updated. You must restart the automation engine using the command `ezdmmn -reconf` for the changes to take effect.

Change the settings temporarily
Perform these steps after ensuring that the automation engine is running:
1. Make the required changes on the tab.
2. Click Apply.
Results:
The new settings take effect immediately. They are not stored in the properties file. If the automation engine is not running, you receive an error message.

Revert to the permanent settings
If you changed the settings temporarily, perform the following steps to revert to the permanent settings defined in the properties file, or when you are unsure which settings are currently active:
1. Invoke the configuration dialog and open the Logger tab. The Logger tab displays the values that are currently set in the properties file.
2. Click Apply to activate the settings.

Results:
The settings take effect immediately.

Controls and fields on the Logger tab:
Maximum log/trace file size
   The file size in kilobytes.

Message logging level:
Error  Logs messages on the error level.
Warning Logs messages on the error and warning levels.
Information Logs messages on the error, warning and informational levels.

Trace logging level:
Off  Collects no trace information.
Minimum Collects trace information on the error level.
Medium Collects trace information on the error and warning levels.
Maximum Provides the message and trace logs and collects additional information on the error, warning, and informational level.

First failure data capture (FFDC) settings:
• Recording level:
  Off  Collects no FFDC information.
  Minimum Provides the message and trace logs and collects additional information on the error level.
  Medium Provides the message and trace logs and collects additional information on the error and warning level.
  Maximum Provides the message and trace logs and collects additional information on the error, warning, and informational level.
• Disk space:
  Maximum disk space
     Specifies the maximum disk space in bytes used by FFDC traces which are written into the FFDC trace directory. The default space is 10485760 byte (10MB).
  Space exceeded policy
     Select what to do if the maximum disk space is exceeded.
• Message IDs:
Filter mode: Initiates the tracing of FFDC data depending on the message IDs listed in Message ID list.

Message ID list: Specifies the message IDs which trigger the tracing of the FFDC data. Wildcard characters can be used (for example, *E for tracing all error messages).

**Saving the basic configuration**

To save your changes to the end-to-end automation manager properties files, click Save on the configuration dialog. Upon completion, the Configuration Update Status window appears, showing the list of configuration files that were updated:

---

If you have configured high availability for the end-to-end automation manager, you must replicate the properties files to the other nodes in the Base component domain (see “Replicating the configuration files” on page 134).

**Configuring high availability for the end-to-end automation manager**

**Notes:**

1. In order to be able to define the policy that makes the end-to-end automation manager high available, the Storage Resource Manager (Storage RM) must be installed on all nodes included in the automation policy.

   **Linux:** StorageRM is installed by default for a Linux installation. The current rpm name is rsct.opt.storagerm-2.4.7.1-07145. The rpm name will change as it carries the build date in it (07145 means that it was built on day 145 of year 07).

   **AIX:** StorageRM is an optional feature of RSCT. The rpm is rsct.opt.storagerm.

   ```
   [root@sapb03] /home/root # lslpp -l rsct.opt.storagerm
   Fileset Level State Description
   """"""
   Path: /usr/lib/objrepos
   rsct.opt.storagerm 2.4.7.1 COMMITTED RSCT Storage Resource Manager
   ```
---
Path: /etc/objrepos
rsct.opt.storagerm 2.4.7.1 COMMITTED RSCT Storage Resource Manager

2. Requests to the end-to-end automation manager are lost when a failover is performed. This is due to the fact that these requests are not persistent.

**Domain setup tab**

Use this tab to specify the parameters required for setting up the Base component domain that will provide high availability for the end-to-end automation manager. The specified parameters will be used to create the Base component domain in the Setup domain task (see.

![Domain setup tab](image)

**Fields on the tab:**

**Domain name**

The name of the Base component domain. To prime the field with the currently defined domain name, click **Query domain**. The domain status (online or offline) is displayed to the right of the field.

**Network tie breaker IP address**

The IP address that is used to set up a network tie breaker. Leave the field empty if you are setting up a three-node Base component domain or if you want to use a different type of tie breaker for a two-node domain. In this case, no network tie breaker will be defined.

To prime the field with the currently defined value, click **Query domain**. Note that when you use **Query domain** to fill this field, the first defined tiebreaker of type "EXEC" will be chosen.

**Node list**

The table lists the nodes of the Base component domain. If the domain is online, clicking **Query domain** will populate the table with the nodes that are online in the domain.

**Table columns:**

**Defined node**

The name of the node.
Automate on node
Indicates whether the end-to-end automation manager is to be automated on the node, in which case it will be included in the automation policy.

Network interface
The name of the network interface on this node.

Possible actions on the tab:
Determining the sequence in which automation selects the node on which the end-to-end automation manager may run
You specify the preferred failover sequence by changing the position of the nodes in the list. To move a node to a different position, select the node from the list and click Up or Down.

Adding, changing, and removing nodes
To change the list of nodes in the automation policy, use the corresponding buttons:

Add  Opens a window for specifying the settings for the node that is to be added to the automation policy.

Change  To modify the settings for a node, select the node, click Change, and modify the settings in the windows that appears.

Remove  To remove a node from the automation policy, select the node, and click Remove.

Automation manager tab
Use this tab to configure the resources that are used to automate the end-to-end automation manager.

Fields on the tab:
Automated resources prefix
The prefix that precedes the names of the resources and groups in the end-to-end automation manager automation policy. The prefix is restricted to ASCII characters.

If you have defined the current automation policy using the old prefix value, you must perform the following steps to change the prefix:
1. Remove the current automation policy.
2. Change the prefix on this tab.
3. Define the automation policy again.

IP address
The virtual IP address that is shared by all nodes in the Base component domain and that is set for the IBM.ServiceIP resource in the end-to-end automation manager automation policy. The virtual IP address must be authorized by your network administrator. To prime the field with the currently defined value, click Query domain.

Netmask
The netmask address that is set for the IBM.ServiceIP resource in the end-to-end automation manager automation policy. Request the address from your network administrator. To prime the field with the currently defined value, click Query domain.

Policy pool tab
Use this tab to specify the parameters required for automating the file system that holds the policy pool. The data is used to create the corresponding file system resource in the automation policy. The policy pool must reside on a file system that is shared by all nodes in the Base component domain. When the automation policy is active, it will be mounted at the specified mount point on the node where the end-to-end automation manager is running.

Fields on the Policy pool tab:

File system type
The type of the policy pool file system to be automated, for example, "jfs", "jfsz", "ext2". To prime the field with the currently defined value, click Query domain.
Mount point
The mount point of the policy pool file system. Click **Browse** to select a directory. If the domain is online, you can click **Query domain** to prime the field with the currently defined value.

Device name
The device name of the policy pool file system. Click **Browse** to select a device. If the domain is online, you can click **Query domain** to prime the field with the currently defined value.

**WebSphere tab**
The tab displays the parameters required for automating the instance of WebSphere Application Server that hosts the end-to-end automation manager. The data is used to create the corresponding resource in the automation policy. The parameters are set by the installer at installation time. Usually, you will not have to change any of the values.

**Notes:**
1. The installation parameters must be identical on all nodes of the Base component domain for the automation policy to work. For example, the path to the profile directory, the Application server port, and the Application server name must be identical on all nodes.
2. To ensure that the Base component can stop WebSphere Application Server, you must add the WebSphere Administrator User ID and its password to the WAS SOAP client properties file. The file is located at /<was_home>/profiles/AppSrv01/properties/soap.client.props. The corresponding entries in this file must look like this:
   ```
   com.ibm.SOAP.loginUserid=<WAS-admin>
   com.ibm.SOAP.loginPassword=<password>
   ```
   You can encrypt this password within the properties file by using the WAS PropFilePasswordEncoder utility. Input parameters for this utility are the properties file path and the password identifier.
   **Example:**
   ```
   /opt/IBM/WebSphere/AppServer1/profiles/AppSrv01/bin/PropFilePasswordEncoder.sh
   /opt/IBM/WebSphere/AppServer1/profiles/AppSrv01/properties/soap.client.props com.ibm.SOAP.loginPassword
   ```
Fields on the WebSphere tab:

**Application server name**
The name of the WebSphere Application Server instance that hosts the end-to-end automation manager.

**Application server port**
The number of the WebSphere Application Server port that is used by the End-to-End Automation Management component.

**Profile directory**
The directory in which the WebSphere Application Server profile for the End-to-End Automation Management component is located. Click **Browse** to navigate to the directory. Click **Browse** to select a directory.

**DB2 tab**
The tab displays the parameters used for automating the DB2 instance that hosts the end-to-end automation management database (EAUTODB). The parameters are set by the installer at installation time. Usually, you will not have to change any of the values.

Note that the installation parameters must be identical on all nodes of the Base component domain for the automation policy to work. For example, the installation directory, the instance owner user ID, and the instance owner mount point must be identical on all nodes.

Controls on the DB2 tab:

**Automate DB2**
Select the check box to enable the entry fields on the tab.

**Installation directory**
Specify the DB2 installation directory or click **Browse** to select a directory.

**Instance owner user ID**
Type the user ID of the owner of the DB2 instance that hosts the EAUTODB database.
Instance owner mount point
Type the mount point of the DB2 instance that hosts the EAUTO DB database or click Browse to select a directory.

Saving the high-availability configuration
To save your entries, click Save on the configuration dialog. Upon completion, the Configuration Update Status window appears, showing the list of configuration files that were updated.

To ensure that the configuration properties are set correctly on all nodes of the domain, you must replicate the configuration files as described below.

Restoring an existing high-availability configuration
To restore a domain configuration from a defined end-to-end automation high availability policy, you can use the Query domain button on the configuration dialog. This retrieves information on most of fields in configuration notebook:

- On the Domain tab:
  - domain name and status (online/offline)
  - list of nodes and network interfaces
  - IP address of the defined network tiebreaker (even it is not the currently active tie breaker, if more than one EXEC tiebreaker is defined, the address of first one)

- On the Automation Manager tab:
  - IP address and netmask of the IBM.ServiceIP resource starting with resource name prefix (for example, "eez-").
  These values are derived from the currently active policy, because they are defined only if "Define policy" is performed and removed if "Remove policy" is performed.

- On the Policy Pool tab:
  - File system type, mount point and device name of the IBM.AgFileSystem starting with resource name prefix (for example, "eez-").
  These values are derived from the currently active policy, because they are defined only if "Define policy" is performed and removed if "Remove policy" is performed.

Replicating the configuration files
If you have configured high availability for the end-to-end automation manager, you must replicate the configuration files to the other nodes in the Base component domain whenever you have made changes to the basic or high-availability configuration. To perform the task, click Replicate on the configuration task launcher. The Replicate Configuration Files window is displayed.

Use this window to distribute (replicate) the configuration files to the remaining nodes in the Base component domain:
1. Select the configuration files you want to replicate or click Select all to select all configuration files in the list.
2. Select the nodes to which the files are to be propagated. If all nodes can be accessed with the same user credentials, click Select all. This is the easiest way to ensure that the configuration is identical on all nodes.
3. Under Target node login, type the user ID and password for the replication target nodes.
4. Start the replication by clicking **Replicate**.

Replication may take a while. While the files are being replicated, the **Replicate** button is indented and grayed-out. When the replication is complete, the replication status of each configuration file is displayed.

**Setting up the domain**

Use this tasks to set up the domain in which the end-to-end automation manager is to be automated. If you will be automating the end-to-end automation manager in a new Base component cluster, you must perform this task before you invoke the high-availability configuration task **Define policy**.

To perform the task, click **Set up domain** on the configuration task launcher. The following window appears, showing the nodes that will make up the domain (the local node and the remote node or nodes, which were specified on the Domain setup tab).

Two actions are performed to set up the domain:

1. **Prepare the remote node or nodes for joining the domain**
   
   To prepare the nodes, specify the user credentials for accessing the nodes. If all nodes can be accessed with the same user credentials, select **Use credentials also for remaining nodes**. To perform the cluster setup, click **Prepare**. Upon completion, a message box is displayed.

2. **Define the domain**
   
   To complete the domain setup, the following commands are performed on the local node:
   
   - **preprnode** - prepares the local node for joining the domain
   - **mkrdomain** - creates the domain definition using the domain name and the nodes that were specified on the Domain setup tab
   - **startrpdomain** - brings the domain online
   
   Note that the Base component must be installed on all nodes that are to be included in the new domain. If other Base domains currently exist, they should be offline.
   
   Upon completion, a message box is displayed.

**Removing the domain**

In order to be able to remove the peer domain definition from all nodes, the domain must be online to the local node.
To remove the domain definition from all nodes in the domain, click **Remove domain** on the task launcher. This invokes the **rmrpdomain** command.

---

### Defining the automation policy for the end-to-end automation manager

Clicking **Define policy** on the configuration dialog task launcher will create the resources with the resource name as described in the table below. Note that if automated resources with the same name exist, they will be changed.

If you specified, for example, the resource-/group prefix name **eez** on the Automation manager tab, the resource group **eez-srvdb2-rg** and the resources and relationships shown in the following table will be created.

**Notes:**

1. Be aware that changing one of these policy elements from outside this dialog, for example by using a console command or by using the sampolicy command, may cause a failure of the remove policy or the define policy task.

2. Activating or deactivating a policy for the IBM Tivoli System Automation for Multiplatforms Base component using the **sampolicy** command may remove existing definitions for the end-to-end automation policy. For example, the definition of one of the resources in the table above may be removed when a new policy for the Base component is activated.

   Therefore, it is recommended that you first save the currently active policy using the **sampolicy -s** command, edit the XML output file, and finally use the command **sampolicy -u** to update the active policy with the changed XML output file. When editing the policy, you must make sure that all definitions for end-to-end automation are preserved and that none of your changes has an undesired effect on the currently active end-to-end automation policy. For details, see the description of the **sampolicy** command in the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*.

**Table 55. Resources in the automation policy for the end-to-end automation manager**

<table>
<thead>
<tr>
<th>Resource name</th>
<th>Resource class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eez-srvdb2-rg</td>
<td>IBM.ResourceGroup</td>
<td>The top-level group that comprises all automated resources</td>
</tr>
<tr>
<td>eez-srv-rg</td>
<td>IBM.ResourceGroup</td>
<td>The group that comprises all resources except of the DB2 related resources</td>
</tr>
<tr>
<td>eez-db2-rg</td>
<td>IBM.ResourceGroup</td>
<td>The group that comprises all DB2 resources</td>
</tr>
<tr>
<td>eez-was-rg</td>
<td>IBM.ResourceGroup</td>
<td>The group that comprises all WebSphere Application Server resources</td>
</tr>
<tr>
<td>eez-engine-rg</td>
<td>IBM.ResourceGroup</td>
<td>The group that comprises all automation manager resources</td>
</tr>
<tr>
<td>eez-ip</td>
<td>IBM.ServiceIP</td>
<td>The virtual IP address used for the WebSphere Application Server</td>
</tr>
<tr>
<td>eez-was-as</td>
<td>IBM.Application</td>
<td>The WebSphere Application server</td>
</tr>
<tr>
<td>eez-engine</td>
<td>IBM.Application</td>
<td>The end-to-end automation manager</td>
</tr>
</tbody>
</table>
Table 55. Resources in the automation policy for the end-to-end automation manager (continued)

<table>
<thead>
<tr>
<th>Resource name</th>
<th>Resource class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eez-shared-mount</td>
<td>IBM.AgFileSystem</td>
<td>The policy-pool for the automation manager; only defined when the policy pool is not harvested by the StorageRM</td>
</tr>
<tr>
<td>eez-db2-rs</td>
<td>IBM.Application</td>
<td>The DB2 server</td>
</tr>
<tr>
<td>eez-db2-rs_mount</td>
<td>IBM.Application</td>
<td>The DB2 filesystem</td>
</tr>
<tr>
<td>db2-rs-dependsOn-db2-rs_mount</td>
<td>IBM.ManagedRelationship</td>
<td>Dependency from DB2 server on the filesystem</td>
</tr>
<tr>
<td>eez-was-as-dependsOn-db2-rs</td>
<td>IBM.ManagedRelationship</td>
<td>Dependency from WebSphere Application Server on DB2</td>
</tr>
<tr>
<td>eez-shared-mount-stopsAfter-engine</td>
<td>IBM.ManagedRelationship</td>
<td>Dependency from the policy pool on the automation manager, only defined if the policy pool is not harvested by the StorageRM</td>
</tr>
<tr>
<td>eez-engine-startsAfter-shared-mount</td>
<td>IBM.ManagedRelationship</td>
<td>Dependency from the automation manager on the policy pool</td>
</tr>
<tr>
<td>eez-engine-startAfter-was-as</td>
<td>IBM.ManagedRelationship</td>
<td>Dependency from the automation manager on the WebSphere application server</td>
</tr>
<tr>
<td>eez-was-as-startsAfter-ip</td>
<td>IBM.ManagedRelationship</td>
<td>Dependency from the WebSphere application server on the virtual IP address</td>
</tr>
<tr>
<td>eez-ip-dependsOn-niequ</td>
<td>IBM.ManagedRelationship</td>
<td>Dependency from the virtual IP address on the network interface</td>
</tr>
<tr>
<td>eez-niequ</td>
<td>IBM.Equivalency</td>
<td>The available network interfaces on each node</td>
</tr>
<tr>
<td>nettb</td>
<td>IBM.TieBreaker</td>
<td>Tie-Breaker defined, if IP address is specified on the domain setup page</td>
</tr>
</tbody>
</table>

Removing the automation policy for the end-to-end automation manager

Clicking Remove policy on the configuration dialog task launcher will remove the resources described in the preceding table. All the resources are first stopped and then removed.

Activating or deactivating a policy for the IBM Tivoli System Automation for Multiplatforms Base component using the sampolicy command may remove existing definitions for the end-to-end automation policy. For example, the definition of one of the resources in the table above may be removed when a new policy for the Base component is activated.
Therefore, it is recommended that you first save the currently active policy using the `sampolicy -s` command, edit the XML output file, and finally use the command `sampolicy -u` to update the active policy with the changed XML output file. When editing the policy, you must make sure that all definitions for end-to-end automation are preserved and that none of your changes has an undesired effect on the currently active end-to-end automation policy. For detailed information, see the description of the `sampolicy` command in the *IBM Tivoli System Automation for Multiplatforms Base Component Reference*. 
Chapter 13. Installing and uninstalling service

Installing service

Installing service means applying corrective service fix packs to release 2.3.0 of IBM Tivoli System Automation for Multiplatforms or upgrading the software release level from release 2.3.0. In this documentation, the service fix packs that you use for updating the End-to-End Automation Management component are referred to as product fix packs.

Note: For some product fix packs, specific interim fixes or fix packs for WebSphere Application Server are required. In such a case, these fixes are available at the location from which you download the product fix pack. They must be installed before the product fix pack is installed. Detailed instructions for installing the fixes are provided in the release notes.

Do not install any WebSphere Application Server interim fixes or fix packs that are not mentioned in the release notes unless you are explicitly advised to do so by Tivoli System Automation support.

Product fix packs and interim fixes are delivered as:
- Self-extracting archives for Windows and AIX
- Archives in TAR-format for Linux

Where to obtain fix packs

Read the release notes to find out which fix packs are required for a release update. The release notes are available on the IBM Tivoli System Automation home page at:


On the page, click Technical Documentation to display the list of available documentation.

The archives can be downloaded from the IBM Tivoli System Automation support site at:


Archive naming conventions

Naming convention for product fix pack archives:

2.3.0-TIV-SAE2E-<platform>-FP<fix_pack_number>..<archive_type>

Naming convention for WebSphere Application Server interim fix archives:

2.3.0-TIV-SAWAS-<platform>-FP<fix_pack_number>..<archive_type>

where
- <platform> represents the platform on which the End-to-End Automation Management component is installed
- <fix_pack_number> represents the fix pack number
- <archive_type> represents the platform-specific file extension of the archive
Example:
This is the tar archive that is used to install product fix pack 1 for IBM Tivoli System Automation for Multiplatforms 2.3 on Linux on POWER platforms: 2.3.0-TIV-SAE2E-PPC-FP0001.tar

Naming conventions of the update installer location

The location at which you find the update wizard program for installing the product fix pack after unpacking an archive has the following syntax:

EEZ23<mf>E2E<platform>/<platform>/<update_wizard_file>

where
- <mf> represents modification level and fix level. For example, for fix pack 2310, the directory is named EEZ2310.
- <platform> represents the platform on which the End-to-End Automation Management component is installed
- <update_wizard_file> represents the update wizard program you use to install the product fix pack

Example:
This is where you find the update wizard after the Linux on POWER archive for fix pack 1 for SA for Multiplatforms 2.3 is unpacked:
EEZ2310E2EPPC/ppc/update

Usage instructions for the platform-specific archives

These are the archives for applying service to the End-to-End Automation Management component.

Windows

Table 56. Windows platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-WIN-FP&lt;fix_pack_number&gt;.exe</td>
<td>The archive is self-extracting. This is where you find the update installer program after unpacking the product fix pack archive: EEZ23&lt;mf&gt;E2EWindows/Windows/setup.exe</td>
</tr>
<tr>
<td>2.3.0-TIV-SAWAS-WIN-FP&lt;fix_pack_number&gt;.exe</td>
<td>The archive is self-extracting. For information about installing WebSphere Application Server interim fixes, refer to the release notes.</td>
</tr>
</tbody>
</table>

AIX

Table 57. AIX platforms

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-AIX-FP&lt;fix_pack_number&gt;.bin</td>
<td>The archive is self-extracting. This is where you find the update installer program after unpacking the product fix pack archive: EEZ23&lt;mf&gt;E2EAIX/AIX/setup.bin</td>
</tr>
</tbody>
</table>
### Table 57. AIX platforms (continued)

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAWAS-AIX-FP&lt;fix_pack_number&gt;.bin</td>
<td>The archive is self-extracting. For information about installing WebSphere Application Server interim fixes, refer to the release notes.</td>
</tr>
</tbody>
</table>

---

### Linux on System x

**Table 58. Linux on System x**

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-I386-FP&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files. This is where you find the update installer program after unpacking the product fix pack archive: EEZ23&lt;mf&gt;E2EI386/I386/setup.bin</td>
</tr>
<tr>
<td>2.3.0-TIV-SAWAS-I386-FP&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files. For information about installing WebSphere Application Server interim fixes, refer to the release notes.</td>
</tr>
</tbody>
</table>

---

### Linux on POWER

**Table 59. Linux on POWER**

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-PPC-FP&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files. This is where you find the update installer program after unpacking the product fix pack archive: EEZ23&lt;mf&gt;E2EPPC/ppc/setup.bin</td>
</tr>
<tr>
<td>2.3.0-TIV-SAWAS-PPC-FP&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files. For information about installing WebSphere Application Server interim fixes, refer to the release notes.</td>
</tr>
</tbody>
</table>

---

### Linux on System z

**Table 60. Linux on System z**

<table>
<thead>
<tr>
<th>Archive name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.0-TIV-SAE2E-S390-FP&lt;fix_pack_number&gt;.tar</td>
<td>For extracting the archive, GNU tar 1.13 or later is required. Use the tar -xf command to extract the files. This is where you find the update installer program after unpacking the product fix pack archive: EEZ23&lt;mf&gt;E2ES390/s390/setup.bin</td>
</tr>
<tr>
<td>2.3.0-TIV-SAWAS-S390-FP&lt;fix_pack_number&gt;.tar</td>
<td>For information about installing WebSphere Application Server interim fixes, refer to the release notes.</td>
</tr>
</tbody>
</table>
Steps for installing a product fix pack

Before you begin:

- Product fix packs are always cumulative.
- Release 2.3.0 must be installed before any product fix pack can be installed.
- To install a product fix pack, you must have root authority.

To install a product fix pack, perform the following steps:

1. Check the release notes to find out which archives are required.
2. Download the archives from the SA for Multiplatforms support site:
   - Archives for WebSphere Application Server fixes: Follow the download instructions provided in the release notes.
   - Archives for product fix packs: Typically, one archive is provided for each platform. Download the archive to a temporary directory.
3. If fixes for WebSphere Application Server must be installed, unpack and install the fixes as described in the release notes.
4. Unpack the product fix pack archive to a temporary directory. For information about how to unpack the archive for your platform, refer to "Usage instructions for the platform-specific archives" on page 140.
5. Before performing the subsequent steps, check the release notes for additional or deviating installation instructions.
6. Change to the directory in which the update wizard program is located. For information on where to find the update wizard program, refer to "Usage instructions for the platform-specific archives" on page 140.
7. Launch the update wizard.
   - When the wizard is launched successfully, the Welcome panel appears.
8. Follow the instructions on the wizard panels to install the product fix pack.

Uninstalling service

Uninstalling service means that you have to uninstall the complete End-to-End Automation Management component as described in Chapter 14, “Uninstalling the End-to-End Automation Management component,” on page 143. After the uninstall procedure is complete, you need to reinstall the component and install the required service level (fix pack level).
Chapter 14. Uninstalling the End-to-End Automation Management component

This section describes how to uninstall the End-to-End Automation Management component. An uninstallation program is provided that removes the components that were installed by the installation wizard.

Note: Uninstall the End-to-End Automation Management component before uninstalling WebSphere Application Server.

Launching the graphical uninstallation program on Windows

To launch the uninstallation program on Windows, you can either issue the command `<EEZ_INSTALL_ROOT>/uninstall/uninstall.exe` at a command prompt or perform the following steps:

1. Open Add or Remove Programs (Start > Control Panel > Add or Remove Programs).

2. On the Add or Remove Programs panel, select Tivoli System Automation for Multiplatforms and click Change/Remove. This brings up the initial panel of the uninstallation program.

Launching the graphical uninstallation program on AIX and Linux

To launch the uninstallation program on AIX and Linux, enter the following command in a shell:

`<EEZ_INSTALL_ROOT>/uninstall/uninstall`

This brings up the initial panel of the uninstallation program.

Using the uninstallation program

Before you begin:

- Before starting the uninstallation of the End-to-End Automation Management component, make sure that the automation engine, the Integrated Solutions Console server, and the WebSphere Application Server “server1” are stopped. For information on how to stop the components, refer to the following sections in the [IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide](#):
  - To stop the automation engine, refer to section "Using the command-line interface of the automation engine".
  - To stop WebSphere Application Server, refer to section "Starting and stopping WebSphere Application Server”.

- During uninstallation, a number of panels may appear prompting you to confirm that specific files are to be deleted. Make sure that the files should be deleted before confirming the deletion.

Perform the following steps to uninstall the End-to-End Automation Management component:
1. Launch the uninstallation program as described in the sections above.

2. Read the information on the first wizard panel and click Next.

3. Specify whether Common Event Infrastructure should be deinstalled and click Next.

4. In the fields on this panel, type the requested information and click Next.
5. The Start Deinstallation panel appears, confirming that the preparations for uninstalling the End-to-End Automation Management component and, should you have opted to deinstall it, the Common Event Infrastructure are complete. Click **Uninstall** to start the uninstallation.

6. Some information panels are displayed while the uninstallation program checks your system for the information it needs for the uninstall. The following figure shows an example.

7. When the uninstallation is complete, a summary window is displayed. To exit the installation program, click **Done**.
Note: If problems were encountered during the unconfiguration step, an error panel appears before the actual uninstallation step (in which the files are removed from the disk). In such a case, do this:

a. On the error panel, click **Save installation log files**.

b. Only if you want to remove all installed file, click Next. Otherwise, click **Cancel** to be able to perform corrective actions and then rerun the uninstallation.
Part 3. Enabling launch-in-context support
Chapter 15. Installing and configuring the IBM
TEC Extension for Tivoli System Automation for
Multiplatforms . . . . . . . . . . . .
Overview. . . . . . . . . . . . . . .
Prerequisites . . . . . . . . . . . . . .
Installing the IBM TEC extension . . . . . . .
Configuring the TEC extension for IBM Tivoli
System Automation for Multiplatforms . . . . .
Adapting the configuration file to your
environment . . . . . . . . . . . . .
Defining a custom button for the Java version of
the TEC Event Console (Java Swing Client) and
the TEC event viewer embedded in TEP . . .
Defining a custom button for the Web version of
the TEC Event Console . . . . . . . . .

149
149
149
150
150
150

151
151

Chapter 16. Setting up Tivoli Enterprise Portal
launch-in-context support . . . . . . . . 153

© Copyright IBM Corp. 2006, 2007

147


Chapter 15. Installing and configuring the IBM TEC Extension for Tivoli System Automation for Multiplatforms

Overview

The IBM TEC Extension for Tivoli System Automation for Multiplatforms (IBM TEC Extension) allows navigating from a displayed event in the Event Console of Tivoli Enterprise Console (TEC Event Console) to the corresponding resource or domain in the SA operations console.

Example usage scenario:
1. An operator sees an event in the TEC Event Console that shows that a Tivoli System Automation resource failed.
2. The operator selects the event and starts the SA operations console for this event.
3. The SA operations console automatically navigates to the resource specified in the event.
4. The operator analyzes the error by checking, for example, the resource status and dependencies.

The IBM TEC Extension can be used for all TEC Event Console setups:
- Java version of the TEC Event Console
- TEC Web console
- TEC event viewer embedded in TEP
  - running using the desktop client interface
  - running using the browser client interface

Prerequisites

To install and use the IBM TEC Extension for Tivoli System Automation for Multiplatforms, the following prerequisites must be met:

TEC version
TEC 3.8 or later

TEC event forwarding
To exploit launch-in-context support from the TEC to the SA operations console, Tivoli System Automation events must be sent to the TEC, which is why you must enable TEC event forwarding for at least one of the following components of Tivoli System Automation for Multiplatforms in your environment:
- Base component for AIX or Linux

For a description on how to enable event forwarding, see the IBM Tivoli System Automation for Multiplatforms Base Component Administrator’s and User’s Guide, section “Using the IBM Tivoli System Automation TEC event interface with the Base component on AIX and Linux”

- End-to-End Automation Management component

You can set up TEC event forwarding during the installation of the component (see “IBM Tivoli Enterprise Console connection configuration data” on page 94) or at any time after the installation is complete (this is
Web browser is required for the Java version of the TEC Event Console

If the Java version of the TEC Event Console is to be used to launch to the SA operations console, a Web browser (Mozilla, Firefox, or Internet Explorer) must be installed on the system where the event console runs.

Installing the IBM TEC extension

For the TEC Web console client, no installation steps are required. You can directly progress to the configuration steps described in “Configuring the TEC extension for IBM Tivoli System Automation for Multiplatforms.”

You only need to perform the installation steps described in this chapter if you are using the Java version of the TEC Event Console or the TEC event viewer embedded in TEP:

- When you are using the Java version of the TEC Event Console, the IBM TEC Extension for System Automation for Multiplatforms needs to be installed on the system where the TEC Event Console runs.
- When you are using the TEC event viewer embedded in the TEP and the TEP is started using the browser client interface, the IBM TEC Extension for System Automation for Multiplatforms needs to be installed on the system where the browser runs.

To install the IBM TEC Extension, perform these steps:
1. Insert the Tivoli System Automation for Multiplatforms product CD into the CD drive.
2. Open a command prompt (Windows) or a command shell (Linux, AIX).
3. Change to the directory ecext on the product CD.
4. Start the installation program, using this command:
   java -jar setup.jar
5. Follow the installation instructions.

Configuring the TEC extension for IBM Tivoli System Automation for Multiplatforms

To enable the launch-in-context feature, complete the following steps:
1. Optional: Adapt the configuration file isc.properties to your environment
2. Define a custom button for the TEC Event Console

See the following sections for a more detailed description of these steps.

Adapting the configuration file to your environment

This is an optional configuration step.

You can use the configuration file isc.properties to configure the host name and port of Integrated Solutions Console. The file is generated by the installer. If you want to change the values specified at the installation, you can change the content of the configuration file. Depending on the TEC Event Console setup, this file is located in the following directory:
TEC Event Console is installed as Java Swing client or TEC event viewer embedded in TEP

The file resides in the same directory where the IBM TEC Extension for System Automation for Multiplatforms is installed.

TEC Web console client

The file can be found in the directory <was_root>/profiles/<server_name>/Tivoli/EEZ

Example of a configuration file:

isc.server = e2eserver1
isc.port = 9060

isc.server is the hostname where the ISC runs which hosts the Tivoli System Automation operations console. isc.port is the port that is used to access the ISC.

Defining a custom button for the Java version of the TEC Event Console (Java Swing Client) and the TEC event viewer embedded in TEP

Perform these steps:
1. Open the Java version of the TEC Event Console.
2. Select Windows > Configuration. Navigate to the console where you want to define the button. Right click Properties.
3. Select the Custom Button entry from the list on the left side of the panel.
4. Click Create Button.
5. Enter a label for the button, for example, “Launch SA Console”, and the location of EEZLaunchSA.

The syntax of the script is:

For Windows:
<path>EEZLaunchSA.bat [<java home>]

Example:
*C:\Program Files\IBM\TECExtension\EEZLaunchSA.bat* C:\IBM\tec_console\jre\bin\n
For AIX and Linux:
<path>EEZLaunchSA.sh [<java home>]

where <path> is the directory in which the TEC Extension for System Automation was installed and the optional parameter <java home> is the Java home directory where the file java.exe can be found. This parameter must end with a / (slash) (Linux and AIX) or with \ (backslash) (Windows).

Java 1.3 or higher is required. If the path contains blanks it must be enclosed in quotes (").

6. Ensure that you have enabled “Event selection required for button action”.

Defining a custom button for the Web version of the TEC Event Console

For the definition of a Web custom button, the Java version of the TEC Event Console is required.

To define the button, do this:
1. Open the Java version of the TEC Event Console.
2. Select Windows > Configuration. Navigate to the console where you want to define the button. Right click Properties.

3. Select the Web Custom Button entry from the list on the left side of the panel.

4. Click Create Button.

5. Enter a label for the button, for example, “Launch SA Console”, and the URL of the Servlet:

   \[ \text{http://<isc_server>:<isc_port>/ibm/EEZUIWebClient/EEZIscUrlBuilderServlet} \]

   where \(<\text{isc_server}>\) is the name of the host where the ISC runs which hosts the Tivoli System Automation operations console and \(<\text{isc_port}>\) is the port that is used to access the ISC.

   **Example:**
   
   \[ \text{http://e2etest:9060/ibm/EEZUIWebClient/EEZIscUrlBuilderServlet} \]

6. Ensure that you have enabled “Event selection required for button action”.


Chapter 16. Setting up Tivoli Enterprise Portal launch-in-context support

If you are using both the SA operations console and Tivoli Enterprise Portal (TEP) for resource monitoring and management, you can set up launch-in-context support for Tivoli Enterprise Portal. Launch-in-context support enables users to launch Tivoli Enterprise Portal workspaces from the SA operations console with a single mouse click.

When Tivoli Enterprise Portal launch-in-context support is configured, a hyperlink becomes available on the General page for first-level automation domains and nodes on the SA operations console, allowing users to open the corresponding Tivoli Enterprise Portal workspaces with a single mouse click.

For launch-in-context support to work properly, a corresponding workspace must be available in Tivoli Enterprise Portal. This also means that the corresponding ITM agents for the objects that are displayed in the SA operations console must be installed, for example, the operating system agent for a displayed system, or the cluster agent for a MSCS cluster, or the corresponding agent for a z/OS sysplex.

The context that is used to find a Tivoli Enterprise Portal workspace is as follows:

<table>
<thead>
<tr>
<th>Selected object in the SA operations console</th>
<th>Context passed during launch</th>
<th>Object searched for to find TEP workspace</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS domain</td>
<td>Sysplex name</td>
<td>managed_system_name=sysplex_name:*</td>
</tr>
<tr>
<td>non-z/OS first-level automation domain</td>
<td>Domain name</td>
<td>managed_system_name=domain_name:*</td>
</tr>
<tr>
<td>z/OS system</td>
<td>Node name</td>
<td>smfid=node_name</td>
</tr>
<tr>
<td>non-z/OS system</td>
<td>Node name</td>
<td>hostname=node_name</td>
</tr>
</tbody>
</table>

In particular, you have to ensure the following:
- For a non-z/OS domain, the first part of the managed system name as displayed in the TEP must match the domain name as configured for the automation adapter of this domain
- For a z/OS system, the system name must be identical to the SMFID
- For a non-z/OS system, the host name that is used in the TEP must match the node name as displayed in the SA operations console.

Here is a description how to change the host name that is used in the TEP:
1. Stop the OS Monitoring agent on the managed system.
2. When the corresponding entry in the TEP navigator goes offline, select the entry, right-click and select **Clear offline entry** from the context menu. The entry should disappear.
3. Open the configuration file for the monitoring agent, which is located in the following path:

\texttt{install\_dir/config/env.config}

Add the following line:

\texttt{CTIRA\_SYSTEM\_NAME=<nodename>}

where \texttt{<nodename>} is the node name exactly as it is presented in the SA operations console.

\textbf{For Windows systems}: Add the CTIRA\_SYSTEM\_NAME variable to the file KNTENV, which is located in \texttt{install\_dir/TMAITM6}.

4. Restart the OS Monitoring agent on the managed system. The system should appear in the TEP navigator with the new name.

To set up launch-in-context support for Tivoli Enterprise Portal, complete the following steps in Integrated Solutions console (EEZAdministrator privileges are required):

1. Open Integrated Solution Console.
2. In the navigation tree, click \textbf{Tivoli System Automation for Multiplatforms > Settings > Tivoli Enterprise launch-in-context support.}
3. In the fields on the page that appears, do this:

\textbf{Enable launch-in-context support for Tivoli Enterprise Portal}
Select to enable launch-in-context support.

\textbf{Server name}
Specify the name of the server on which Tivoli Enterprise Portal runs.

\textbf{Port number}
Specify the port number of the server on which Tivoli Enterprise Portal runs. The default port number is 1920.

4. Click \textbf{OK} to save the configuration.
Part 4. Installing and configuring the end-to-end automation adapters

Chapter 17. Overview ........................................... 157

Chapter 18. Configuring the end-to-end automation adapter of the Base component of IBM Tivoli System Automation for Multiplatforms .................................................................. 159
Automating the end-to-end automation adapter ........................................... 161
Invoking the end-to-end automation adapter configuration dialog ............ 161
Configuring the end-to-end automation adapter ......................................... 163
  Adapter tab ........................................................................ 163
  Host using adapter tab .......................................................... 165
  Automation tab ..................................................................... 167
  Security tab ......................................................................... 170
  Logger tab .......................................................................... 172
  Saving the configuration.......................................................... 174
Replicating the end-to-end automation adapter configuration files to other nodes in the domain ........................................... 175
Defining the end-to-end automation adapter policy ..................................... 176
Removing the adapter automation policy .................................................. 177
Controlling the end-to-end automation adapter ....................................... 177

Chapter 19. Installing and configuring the HACMP adapter .......................... 179
Installing the HACMP adapter .......................................................... 179
  Packaging ........................................................................... 179
  Installation prerequisites ......................................................... 179
  Using SMIT to install the adapter ........................................... 179
Automating the HACMP adapter ........................................................... 180
Configuring the HACMP adapter .......................................................... 180
  Invoking the HACMP adapter configuration dialog .......................... 181
  Configuring the HACMP adapter ............................................. 182
    Adapter tab ....................................................................... 182
    Host using adapter tab ......................................................... 184
    Automation tab ................................................................... 186
    Security tab ...................................................................... 187
    Logger tab ........................................................................ 189
    Saving the configuration........................................................ 191
Replicating the HACMP adapter configuration files to other nodes in the domain ........................................... 192
Defining the HACMP adapter automation policy ...................................... 193
Removing the HACMP adapter automation policy .................................... 193
Verifying the HACMP adapter configuration .......................................... 194
Controlling the HACMP adapter ........................................................... 194

Planning and preparing for the MCSI adapter ......................................... 198
  Packaging ........................................................................... 198
  Installation prerequisites ......................................................... 198
  Planning and preparing for high availability ..................................... 199
  Installation directories ............................................................. 199
Installing the MCSI adapter .................................................................. 199
  Using the installation wizard to install the MCSI adapter .................. 199
  Installing the adapter in silent mode .......................................... 201
Configuring the MCSI adapter ............................................................ 201
  Invoking the MCSI adapter configuration dialog ............................ 201
  Configuring the MCSI adapter ................................................. 202
    Adapter tab ....................................................................... 202
    Host using adapter tab ......................................................... 204
    Security tab ...................................................................... 205
    Logger tab ........................................................................ 206
    Saving the configuration........................................................ 208
Replicating the MCSI adapter configuration files to other nodes ......... 209
Providing high availability for the MCSI adapter .................................. 210
Verifying the installation and configuration ........................................... 215
Uninstalling the MCSI adapter ............................................................. 216

Chapter 21. Installing and configuring the VERITAS Cluster Server adapter ........................................... 217
Installing the VCS adapter ............................................................. 217
  Packaging ........................................................................... 217
  Installation prerequisites ......................................................... 217
  Using the installation wizard to install the VCS adapter ................. 217
Automating the VCS adapter ............................................................ 218
Configuring the VCS adapter ........................................................... 218
  Invoking the VCS adapter configuration dialog ............................ 220
  Configuring the VCS adapter ................................................. 221
    Adapter tab ....................................................................... 221
    Host using adapter tab ......................................................... 222
    Automation tab ................................................................... 224
    Security tab ...................................................................... 226
    Logger tab ........................................................................ 227
    Saving the configuration........................................................ 229
Replicating the VCS adapter configuration files to other nodes in the domain ........................................... 230
Defining the VCS adapter automation policy ...................................... 231
Removing the VCS adapter automation policy .................................... 231
Verifying the VCS adapter configuration .......................................... 231
Controlling the VCS adapter ........................................................... 232

© Copyright IBM Corp. 2006, 2007
Chapter 17. Overview

The End-to-End Automation Management component of IBM Tivoli System Automation for Multiplatforms can be used to automate the operation of resources within heterogeneous environments (called first level automation domains) that each have a local automation technology of their own. Each first-level domain is connected to the end-to-end automation manager or an operations console by an end-to-end automation adapter.

The purpose of an automation adapter is to

- Monitor resources within its first-level automation domain
- Propagate resource attribute changes to the end-to-end automation manager.
- Start and stop resources within the first-level automation domain by request of the end-to-end automation manager or an operator.
- Provide information for resources that are available within the first-level automation domain.

The end-to-end automation adapter uses the Tivoli Event Integration Facility (EIF) to communicate with the end-to-end automation manager.

The chapters in this section describe how you install and configure the automation adapters for IBM Tivoli System Automation for Multiplatforms:

- **Chapter 18, “Configuring the end-to-end automation adapter of the Base component of IBM Tivoli System Automation for Multiplatforms,” on page 159** describes how you configure the automation adapter for the Base component. The adapter is installed automatically when you install the Base component.
- **Chapter 19, “Installing and configuring the HACMP adapter,” on page 179** describes how you install and configure the HACMP adapter, which is shipped with the End-to-End Automation Management component.
- **Chapter 20, “Installing and configuring the MSCS adapter,” on page 197** describes how you install and configure the MSCS adapter, which is shipped with the End-to-End Automation Management component.
- **Chapter 21, “Installing and configuring the VERITAS Cluster Server adapter,” on page 217** describes how you install and configure the VCS adapter, which is shipped with the End-to-End Automation Management component, on Solaris/SPARC systems.
Chapter 18. Configuring the end-to-end automation adapter of the Base component of IBM Tivoli System Automation for Multiplatforms

The following sections describe how to configure the end-to-end automation adapter of the Base component.

You need to configure the end-to-end automation adapter when you use the End-to-End Automation Management component of IBM Tivoli System Automation for Multiplatforms or if you want to operate automated resources directly from an operations console. (For information about the End-to-End Automation Management component, see the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide).

Note: To use the Base component operations console or end-to-end automation management, Base component object names, for example, group names, resource names, and descriptions, must not contain the following characters:
" (double quotation mark), ' (single quotation mark), ; (semicolon), $ (dollar sign), / (slash)

The online helps provided with the System Automation for Multiplatforms end-to-end automation adapter configuration dialog also provide useful information about using and configuring the end-to-end automation adapter.

The following figure shows in which environments the end-to-end automation adapter can operate and what needs to be configured for the end-to-end automation adapter:
Figure 9 shows that you have two adapter configuration alternatives which are mutually exclusive:

- You can configure the adapter for the operations console of the Base component of IBM Tivoli System Automation. In this case, the adapter is accessed directly by the operations console, without communicating via the end-to-end automation manager. This operations console mode is referred to as direct access mode.

- If the End-to-End Automation Management component is installed, you can configure the adapter for end-to-end automation management. This is required if you want to implement end-to-end automation and run the operations console in end-to-end automation mode, or if you want to use the operations console in first-level automation mode. For more information on end-to-end automation management and these console modes, refer to the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide.
Automating the end-to-end automation adapter

If the IBM Tivoli System Automation for Multiplatforms Base component cluster consists of more than one node, the end-to-end automation adapter must be automated. (For a description of how this can be achieved, refer to “Automation tab” on page 167)

When the adapter is automated, it can run on any node that is online in the cluster. This is necessary because the adapter is connected to two components as shown in Figure 9 on page 160.

1. The event publisher, which sends events to the adapter, for example, if the state of a resource changes. The event publisher runs on the master node. The master node can change at any time, for example, if a node goes down or a severe error condition occurs. This would be no problem if the adapter only received events from the event publisher because the event publisher will silently move to a new node. However, the adapter also communicates with the so-called host using the adapter.

2. The host using the adapter, which is either the operations console of the Base component or the end-to-end management component of IBM Tivoli System Automation. The adapter both sends events on resource changes to the host using the adapter and receives requests from the host using the adapter.

This means that the adapter must be able to always receive requests from both the host using the adapter and from the event publisher. To achieve this, the event publisher and the host using the adapter must access the adapter over a unique IP address which must be entered on the automation tab as described in “Automation tab” on page 167. This IP address must be requested from the system administrator.

This is what can happen if the adapter is running on the master node but has not been automated:

1. If the node on which the adapter runs goes down, the host using the adapter cannot access it anymore. Therefore it is not possible to learn how the automated resources behaved.

2. Although resources change their state, the operations console or end-to-end management may not show these changes. Select ‘Refresh’ to get the most recent state in the operations console displayed. The reason of this behavior is that the event publisher silently moved to another node.

The following sections describe how to configure and work with the end-to-end automation adapter.

Invoking the end-to-end automation adapter configuration dialog

The end-to-end automation adapter can be configured with the cfgsamadapter utility.

Notes:

1. No end-to-end automation adapter and no cfgsamadapter is available for the Base component running on Windows.

2. The cfgsamadapter utility is an X-application and must be used from a workstation with Xserver capabilities. This could be one of your cluster nodes, if the X11 optional feature is installed on that node.
3. On AIX systems, the following requirements must be met for the end-to-end automation adapter installation:
   • The 32-bit version of Java 1.4 or Java 5 SR5 must be installed.
   • SSL/SSH packages must be installed and the sshd subsystem must be running to be able to complete the Replication task of the adapter configuration.

4. To use the System Automation for Multiplatforms adapter configuration dialog, you must be logged on to the system with the user ID root or you must have write access to the directories /etc/opt/IBM/tsamp/sam/cfg and /etc/Tivoli.

Issue the `cfgsamadapter` command to invoke the System Automation for Multiplatforms adapter configuration dialog. The main panel of the dialog is displayed:

![Figure 10. Main panel of the end-to-end automation adapter configuration dialog](image)

This dialog lets you perform the following tasks:
1. Configure the end-to-end automation adapter (see page 163)
2. Replicate the end-to-end automation adapter configuration files to other nodes (see page 175)
3. Define the end-to-end automation adapter automation policy to create the resources required to automate the adapter (see page 176)
4. Remove the end-to-end automation adapter automation policy (see page 177)
Configuring the end-to-end automation adapter

On the main panel of the configuration dialog, click Configure to display the configuration tabs that are described in the following sections. In the following description, the term Host using the adapter is used to refer to either the end-to-end automation manager or the Base component operations console.

Adapter tab

On the Adapter tab, you can configure the adapter host.

![Automation Adapter Configuration](image)

**Figure 11. System Automation for Multiplatforms end-to-end adapter configuration**

**Fields and controls on the Adapter tab:**

Host name or IP address

Host name of the node where the adapter runs if the adapter is not automated.

If you select to automate the adapter, the value is updated automatically with the value you specify in the field Adapter IP address on the Automation tab (see "Automation tab" on page 167). In this case, do not change the value in the field.

Request port number

The port on which the adapter listens for requests from the host using the adapter. The default port is 2001.

Event port number

The port on which the end-to-end automation adapter listens for events from the first level automation manager. The default port is 5539.
Policy pool location
   The fully qualified name of the directory in which the XML policy files are stored. Any policy that you want to activate from the operations console must reside in this directory.

Clicking Advanced lets you specify the adapter runtime behavior:

Adapter stop delay
   The number of seconds by which the adapter stop is delayed to allow the adapter to properly deliver the domain leave event. The default value is 5. You may need to increase the value on slow systems. Valid values are 3 through 60.

Remote contact activity interval
   The time period, in seconds, after which the adapter will stop if it was not contacted by the host using the adapter, which periodically contacts the adapter to check if it is still running. The default value is 360. If a value other than 0 is specified, the interval must be a multiple of the check interval.
   When the value is set to 0, the adapter continuously runs and never stops. This is the recommended setting for adapters that are connected to a Base component operations console, because otherwise the adapter will be stopped whenever the operations console is stopped.

Initial contact retry interval
   The time period, in minutes, within which the adapter will attempt to contact the host using the adapter until it succeeds or the specified time has elapsed. The default value is 0, which means that the adapter will attempt to contact the host using the adapter indefinitely.

EIF reconnect attempt interval
   The time period, in seconds, that the adapter will wait before it attempts to reestablish the connection to the host using the adapter after the connection was interrupted. The default value is 30.
**Host using adapter tab**

Use the Host using adapter tab to determine which host the adapter connects to and to specify the required information.

The end-to-end automation adapter can be configured to connect to one of these hosts:
- An end-to-end automation management host
- A Base component operations console, which runs in direct-access mode

An adapter can only connect to a single host, the configurations are mutually exclusive.

![Automation Adapter Configuration](image)

*Figure 12. Host using adapter tab*

**Fields and controls on the Host using adapter tab:**

Configure end-to-end management host:

**Host name or IP address**

The name or IP address of the host on which the end-to-end automation manager runs. The port number specified here must match the port number specified as event port number when configuring the domain of the end-to-end automation manager.

**Event port number**

The port on which the end-to-end automation manager listens for events from the end-to-end automation adapter. The default port is 2002.

Configure direct access operations console:
Host name or IP address
The name or IP address of the host on which the operations console runs.

Event port number
The port on which the operations console listens for events from the end-to-end automation adapter. The default port is 2002.
Automation tab

This tab lets you configure the adapter automation policy. This allows you to make the end-to-end automation adapter highly available, meaning that if the node on which the adapter runs breaks down, the adapter will be restarted on another node in the domain.

**Note:** All nodes where the adapter can run must be accessible using the same user ID and password.

Automate adapter in system automation domain
Select this check box if the end-to-end automation adapter is running in an RSCT peer domain with more than one node. See the section which discusses automation on tab 161.

Query domain
Provided that the node on which the configuration dialog runs is in the RSCT peer domain, this queries the current automation policy. If the domain is online, all nodes that are online are shown in the **Defined nodes** table. This table provides the following information:
- Defined node
  If the RSCT peer domain is online, all nodes that are online are shown here
- Automate on node
  Indicates if the adapter is automated on this node.
- Network interface
  Name of the network interface used for requests from the **host using the adapter**.

---

*Figure 13. Automating the adapter*

Chapter 18. Configuring the end-to-end automation adapter  167
The buttons at the bottom of the table let you perform the following:

- **Up**
  Moves the selected node one position up in the node sequence. The position determines the order in which automation selects the node on which the end-to-end automation adapter may run.

- **Down**
  Moves the selected node one position down in the node sequence. The position determines the order in which automation selects the node on which the end-to-end automation adapter may run.

- **Add**
  Displays the Add node for adapter automation panel which lets you define the name of the node to be added, determine if the node is to be added to automation of the adapter, and lets you enter the name of the network interface.

- **Remove**
  Removes the selected node from the list. This means that the end-to-end automation adapter must not be started on that node.

- **Change**
  Displays the Change node for adapter automation panel which lets you change the name of the node, add or remove the node from automation of the adapter, and lets you change the name of the network interface.

### Automated resources prefix

This shows the prefix of the resource or resource groups names in the automation policy.

The prefix can be changed.

It is restricted to ASCII characters; the following characters cannot be used:

- " (double quote), ' (single quote), ; (semicolon), $ (dollar), / (slash)

Note that if the end-to-end adapter policy has been defined using the current prefix, you must remove this policy before changing the prefix.

For more information about defining the adapter automation policy, refer to "Defining the end-to-end adapter automation policy" on page 176.

### Adapter IP address

Regardless on which node it runs, the end-to-end automation adapter uses this address to listen for requests and receive requests from the host using the adapter. It is an IP address which will be used as a ServiceIP resource to automate the adapter. You must obtain this IP address from your network administrator and it must neither be an actual host address nor localhost.

### Netmask

The netmask that is used to define the ServiceIP resource in the adapter automation policy. Request a value from your network administrator.

**Note:** When you click **Save** after specifying an IP address in the field **Adapter IP address**, the following message may be displayed:
The message informs you that the IP addresses on the Adapter and Automation tabs differ and asks you to confirm that the IP address on the Adapter tab is to be updated with the value you specified on the Automation tab. Click Yes to confirm the change.
Security tab

This tab lets you configure the security for the interface between the end-to-end automation adapter and the end-to-end management host.

Select the Enable SSL check box if you want to use the Secure Socket layer (SSL) protocol. If checked, the following entry fields must be completed.

- **Truststore**: Name of the truststore file used for SSL. The file name may contain multiple period characters. Click **Browse** to select a file.
- **Keystore**: Name of the keystore file used for SSL. The file name may contain multiple period characters. Click **Browse** to select a file.
- **Keystore password**: Password of the keystore file. The password is required if a keystore file was specified. Click **Change** to change the password.

**Note:** If the truststore is in different file than keystore, the passwords for the files must be identical.

- **Keystore alias**: Alias name of the certificate to be used by the server. If not specified, the keystore file must contain only one entry which is the one to be used.

Also select the Enforce user authentication check box to enable the authentication of the user with Pluggable Access Module (PAM).

- **PAM Service**: The name of a file in the directory `/etc/pam` (SUSE), or an entry in file `/etc/pam.d` (RedHat), or an entry in file `/etc/pam.conf` (AIX) that determines which checks are made to authenticate a user. On
AIX 5.2, you may have to perform the steps described for AIX 5.2 in Chapter 1, “Installing the Base component for AIX and Linux,” section “Preparing for installation” on page 6.
Logger tab

Use the Logger tab to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the configuration file.

On the Logger tab, you can perform the following tasks:

**Change the settings permanently**

Perform these steps:
1. Make the required changes on the tab.
2. Click **Save**.

**Results:**
The settings in the configuration file are updated. You must restart the adapter for the changes to take effect.

**Change the settings temporarily**

Perform these steps after ensuring that the adapter is running:
1. Make the required changes on the tab.
2. Click **Apply**.

**Results:**
The new settings take effect immediately. They are not stored in the configuration file. If the adapter is not running, you receive an error message.

**Revert to the permanent settings**

If you changed the settings temporarily, perform the following steps to
revert to the permanent settings defined in the configuration file, or when you are unsure which settings are currently active for the adapter:

1. Invoke the configuration dialog and open the Logger tab. The Logger tab displays the values that are currently set in the configuration file.
2. Click **Apply** to activate the settings.

**Results:**
The settings take effect immediately. If the adapter is not running, you receive an error message.

**Controls and fields on the Logger tab:**

**Maximum log/trace file size**
The file size in kilobytes.

**Message logging level:**
- **Error** Logs messages on the error level.
- **Warning** Logs messages on the error and warning levels.
- **Information** Logs messages on the error, warning and informational levels.

**Trace logging level:**
- **Off** Collects no trace information.
- **Minimum** Collects trace information on the error level.
- **Medium** Collects trace information on the error and warning levels.
- **Maximum** Provides the message and trace logs and collects additional information on the error, warning, and informational level.

**First failure data capture (FFDC) settings:**
- **Recording level:**
  - **Off** Collects no FFDC information.
  - **Minimum** Provides the message and trace logs and collects additional information on the error level.
  - **Medium** Provides the message and trace logs and collects additional information on the error and warning level.
  - **Maximum** Provides the message and trace logs and collects additional information on the error, warning, and informational level.
- **Disk space:**
  - **Maximum disk space** Specifies the maximum disk space in bytes used by FFDC traces which are written into the FFDC trace directory. The default space is 10485760 byte (10MB).
  - **Space exceeded policy** Select what to do if the maximum disk space is exceeded.
- **Message IDs:**
  - **Filter mode** Initiates the tracing of FFDC data depending on the message IDs listed in Message ID list.
Message ID list:

Specifies the message IDs which cause the tracing of the FFDC data. Wildcards like *E, meaning all error messages, are allowed.

**Saving the configuration**

Click **Save** on the configuration dialog to save your changes to the adapter configuration files. Upon completion, the configuration update status panel appears, showing the list of configuration files that were updated. This is depicted in Figure 16.

**Notes:**

1. When you changed the Adapter IP address on the Automation tab, the message described in the note on page 168 may be displayed. Click **Yes** to confirm the change and to save the new configuration to the configuration files.
2. When entries are missing or a value you have entered is out of range (for example, a port number), an error message is displayed.
3. If you made changes on the Automation tab, a message appears reminding you to launch the Define automation policy task.
4. If not noted otherwise, you must restart the adapter for the changes to become effective.

![Configuration Update Status](image)

Figure 16. Configuration update status panel
Replicating the end-to-end automation adapter configuration files to other nodes in the domain

Click Replicate on the main panel of the configuration dialog (see Figure 10 on page 162). The following panel is displayed:

![Replicate Configuration Files](image)

Figure 17. System Automation for Multiplatforms replicate configuration files panel

Use this window to distribute (replicate) the end-to-end automation adapter configuration itself or configuration updates to the remaining nodes in the RSCT peer domain:

1. Select the configuration files you want to replicate or click Select all to select all configuration files in the list.
2. Click Select all below the list of replication target nodes. This ensures that the adapter configuration is identical on all nodes.
3. Enter the user ID and password for the target nodes you want to replicate the files to.
4. Start the replication by clicking Replicate.

Replication may take a while. While the files are being replicated, the Replicate button is indented and grayed-out. When the replication is complete, the replication status of each configuration file is displayed.
Defining the end-to-end adapter automation policy

Clicking Define on the main panel of the configuration dialog (see Figure 10 on page 162) will create the resources with the resource name (Resource-/group prefix) as described on page 168. Note that if automated resources with the same name existed, they will be removed before creation of the new ones.

If you specified, for example, the resource-/group prefix name samadapter, the resource group samadapter-rg, and the resources and relationships shown in the following table will be created.

<table>
<thead>
<tr>
<th>Resource name</th>
<th>Resource class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>samadapter-rg</td>
<td>IBM.ResourceGroup</td>
<td>The resource group that comprises all automated resources.</td>
</tr>
<tr>
<td>samadapter</td>
<td>IBM.Application</td>
<td>The samadapter application itself.</td>
</tr>
<tr>
<td>samadapter-ip</td>
<td>IBM.ServiceIP</td>
<td>The virtual IP address on which the adapter can be accessed from the host using the adapter and the EIF event publisher.</td>
</tr>
<tr>
<td>samadapter-nieq</td>
<td>IBM.Equivalency</td>
<td>The available network interfaces on each node.</td>
</tr>
<tr>
<td>samadapter-on-ip</td>
<td>IBM.ManagedRelationship</td>
<td>The dependency of samadapter on the IP address.</td>
</tr>
<tr>
<td>samadapter-ip-on-nieq</td>
<td>IBM.ManagedRelationship</td>
<td>The dependency of the IP address on the network interface.</td>
</tr>
</tbody>
</table>

When you click Define, the button may stay indented for minutes until the resources have been removed, the cluster is synchronized, the new resources are created, and the cluster is synchronized again. The dialog will not repaint after it has been covered and uncovered. Eventually, the results of the commands are displayed in a pop-up window.

Note: Activating a complete (not incremental) policy, or deactivating a policy for the IBM Tivoli System Automation for Multiplatforms Base component using the sampolicy command may remove existing definitions for the end-to-end adapter automation policy, or definitions that are referenced by an end-to-end automation policy. For example, the definition of a resource that is referenced in an end-to-end automation policy may be removed when a new policy for the Base component is activated.

Therefore, it is recommended that you first save the currently active policy using the sampolicy -s command, edit the XML output file, and finally use the command sampolicy -u to update the active policy with the changed XML output file. When editing the policy, you must make sure that all definitions for end-to-end adapter automation are preserved and that none of your changes has an undesired effect on the currently active end-to-end automation policy.
Removing the adapter automation policy

You typically use the Remove function before you change the name prefix of the automated resources (see page 168). When the adapter is automated and you deselect the check box Automate adapter in system automation domain on the Automation tab, you receive a message reminding you to remove the automated resources for the adapter.

Clicking Remove on the main panel of the configuration dialog will remove the resources shown in Table 62 on page 176. If the end-to-end automation adapter is still running, it is stopped before the automated resources are removed.

When you click Remove, the button may stay indented for minutes until resources have been removed and the cluster has been synchronized. Eventually, the results of the commands are displayed in a pop-up window.

Controlling the end-to-end automation adapter

You use the samadapter command to start, stop, and monitor the adapter.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>samadapter status</td>
<td>Checks if the adapter is running and returns the RSCT return code for the operational state (OpState):</td>
</tr>
<tr>
<td></td>
<td>0 Unknown. The adapter status cannot be determined.</td>
</tr>
<tr>
<td></td>
<td>1 Online. The adapter is running.</td>
</tr>
<tr>
<td></td>
<td>2 Offline. The adapter is not running.</td>
</tr>
<tr>
<td>samadapter start</td>
<td>Starts the adapter if it is not running:</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is automated, the command issues a request to start the adapter on the preferred node. The command returns when the request has been submitted.</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is not automated, it is started on the node on which the command was issued.</td>
</tr>
<tr>
<td>samadapter stop</td>
<td>Stops the adapter if it is running:</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is automated, the command issues a request to stop the adapter on the node where it is currently active. The command returns when the request has been submitted.</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is not automated, it is stopped on the node on which the command is issued.</td>
</tr>
</tbody>
</table>
Chapter 19. Installing and configuring the HACMP adapter

The following topics describe how to install and configure the HACMP adapter.

Installing the HACMP adapter

Packaging

The HACMP adapter is shipped with the End-to-End Automation Management component. The name of the installp package you use for installing the adapter is hac.adapter. This is where you find the installation package:

- **CD:**
  You install the adapter from the CD "Tivoli System Automation for Multiplatforms - End-to-End component, Automation Adapters all platforms". The installation package is available in the installation source directory EEZ2300Adapters/EEZ2300HACMP/AIX.

- **Electronic distribution:**
  If you obtain the End-to-End Automation Management component through electronic distribution, you use the following archive to install the HACMP adapter:
  - Deliverable name: C106FML.bin
  - Installation source directory: EEZ2300Adapters/EEZ2300HACMP/AIX

Installation prerequisites

Note that the HACMP adapter can only be connected to an End-to-End Automation Management component V2R2 or later.

The system on which you are installing the adapter must meet the following installation prerequisites:

- Required minimum HACMP release level: 5.3.0.5 (PTF5)
- The HACMP adapter must not run on a node in the RSCT peer domain. If the node on which the adapter is to run previously was an RSCT peer domain node, the following actions must be taken prior to installing the adapter:
  1. The environment variable CT_MANAGEMENT_SCOPE, which is set to 2 for the RSCT peer domain, must be unset.
  2. The RSCT registry must be cleared using the command /usr/sbin/rsct/install/bin/recfgct
- The 32-bit version of Java 1.4 or Java 5 SR5 must be installed.
- SSL/SSH packages must be installed and the ssdh subsystem must be running to be able to complete the Replication task of the adapter configuration

Using SMIT to install the adapter

You find the package in the directory on the CD or in the electronic deliverable as described in "Packaging."

Package name: hac.adapter. Use the SMIT interface to install the adapter.

The HACMP adapter installation directory is /opt/IBM/tsamp/eez/hac
Note: Do not change the installation directory or the configuration directory
(/etc/opt/IBM/tsamp/eez/hac/cfg). Otherwise, the HACMP adapter cannot
be run because it relies on fixed paths.

After installing the adapter it must be configured as described in the remaining
sections of this chapter.

Automating the HACMP adapter

If the HACMP cluster consists of more than one node, the HACMP adapter must
be automated for the following reasons:

• The host using the adapter must be able to reach the adapter always through the
  same service IP without reconfiguration.

• If the node on which the adapter runs goes down or the HACMP cluster
  services on that node are stopped, the adapter must move to another available
  node in the cluster to resume the connection with the host using the adapter.

For more information about automating HACMP adapters using the adapter
configuration dialog, see “Automation tab” on page 186.

Configuring the HACMP adapter

The following figure shows in which environments the HACMP adapter can work
and what needs to be configured for the adapter.
Figure 18 shows that you have two adapter configuration alternatives which are mutually exclusive:

- You can configure the adapter for the operations console of the Base component of IBM Tivoli System Automation. In this case, the adapter is accessed directly by the operations console, without communicating via the end-to-end automation manager. This operations console mode is referred to as **direct access mode**.

- If the End-to-End Automation Management component is installed, you can configure the adapter for end-to-end automation management. This is required if you want to implement end-to-end automation and run the operations console in end-to-end automation mode or if you want to use the operations console in first-level automation mode. For more information on end-to-end automation management and these console modes, refer to the **IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide**.

### Invoking the HACMP adapter configuration dialog

The HACMP adapter can be configured with the `cfghacadapter` utility. The utility is an X-application that must be used from a workstation with Xserver capabilities. This could be one of your cluster nodes, if the X11 optional feature is installed on that node.
To use the HACMP adapter configuration dialog you, must be logged in to the system with the user ID root or you must have write access to the directory 
/etc/opt/IBM/tsamp/eez/hac/cfg.

Issue the cfhacadapter command to invoke the configuration dialog.

The main panel of the dialog is displayed:

![Main panel of the HACMP adapter configuration dialog](image)

Figure 19. Main panel of the HACMP adapter configuration dialog

The dialog lets you perform the following tasks:
1. Configure the HACMP adapter.
2. Replicate the HACMP adapter configuration files to other nodes.
3. Define the HACMP adapter automation policy to create the resources required to automate the adapter.
4. Remove the HACMP adapter automation policy.

**Configuring the HACMP adapter**

On the main panel of the configuration dialog, click Configure to display the configuration tabs that are described in the following sections.
In the following description, the term **Host using the adapter** is used to refer to either the end-to-end automation manager or the Base component operations console.

**Adapter tab**

On the Adapter tab, you can configure the adapter host.
Fields and controls on the Adapter tab:

Automation adapter host:

Host name or IP address

Host name or service IP label of the node where the adapter runs.

On initial invocation, the field contains the value the command `hostname` would return.

If you are automating the adapter, leave the value unchanged. The value will be updated automatically with the value you specify in the field Service IP label on the Automation tab (see "Automation tab" on page 186).

Request port number

The port on which the adapter listens for requests from the host using the adapter. The default port is 2001.

Clicking Advanced lets you specify the adapter runtime behavior:

Adapter stop delay

The number of seconds by which the adapter stop is delayed to allow the adapter to properly deliver the domain leave event. The default value is 5. You may need to increase the value on slow systems. Valid values are 3 through 60.

Remote contact activity interval

The time period, in seconds, after which the adapter will stop if it was not contacted by the host using the adapter, which periodically contacts the adapter to check if it is still running. The
default value is 360. If a value other than 0 is specified, the interval must be a multiple of the check interval.

When the value is set to 0, the adapter continuously runs and never stops. This is the recommended setting for adapters that are connected to a Base component operations console, because otherwise the adapter will be stopped whenever the operations console is stopped.

Initial contact retry interval
The time period, in minutes, within which the adapter will attempt to contact the **host using the adapter** until it succeeds or the specified time has elapsed. The default value is 0, which means that the adapter will attempt to contact the **host using the adapter** indefinitely.

EIF reconnect attempt interval
The time period, in seconds, that the adapter will wait before it attempts to reestablish the connection to the **host using the adapter** after the connection was interrupted. The default value is 30.

**Host using adapter tab**
Use the Host using adapter tab to determine which host the adapter connects to and to specify the required information.

The HACMP adapter can be configured to connect to one of these host:
- An end-to-end automation management host
- A Base component operations console, which runs in direct-access mode

An adapter can only connect to a single host, the configurations are mutually exclusive.
Fields and controls on the Host using adapter tab:

Configure end-to-end management host:

Host name or IP address
The name or IP address of the host on which the end-to-end automation manager runs. The port number specified here must match the port number specified as event port number when configuring the domain of the end-to-end automation manager.

Event port number
The port on which the end-to-end automation manager listens for events from the HACMP adapter. The default port is 2002.

Configure direct access operations console:

Host name or IP address
The name or IP address of the host on which the operations console runs.

Event port number
The port on which the operations console listens for events from the HACMP adapter. The default port is 2002.
Automation tab

Figure 22. Automation tab of the HACMP configuration dialog

This tab lets you configure the adapter automation policy. This allows you to make the end-to-end automation adapter highly available, meaning that if the node on which the adapter runs breaks down, the adapter will be restarted on another node in the domain.

Note: All nodes where the adapter can run must be accessible using the same user ID and password.

Fields and controls on the Automation tab:

Automate adapter in first-level automation domain
Select this check box (see also “Automating the HACMP adapter” on page 186).

Query domain If the configuration dialog runs on a node in the HACMP cluster, click Query domain to query the current automation policy from the HACMP cluster. If the automation policy for the adapter is not yet defined but the cluster is up, at least all nodes that are online are shown in the Defined nodes table. This table provides the following information:

- Defined node
  The list of defined nodes.
- Automate on node
  Indicates if the adapter is automated on this node.

The buttons at the bottom of the table let you perform the following tasks:
• Up
  Moves the selected node one position up in the node sequence. The position determines the order in which automation selects the node on which the adapter may run.

• Down
  Moves the selected node one position down in the node sequence. The position determines the order in which automation selects the node on which the adapter may run.

• Add
  Displays the Add node for adapter automation panel which lets you define the name of the node to be added and determine if the node is to be added to automation of the adapter.

• Remove
  Removes the selected node from the list. This means that the adapter must not be started on that node.

• Change
  Displays the Change node for adapter automation panel which lets you change the name of the node and add or remove the node from automation of the adapter.

HACMP root directory
  Shows the root directory where HACMP is installed.

Automated resources prefix
  The prefix that is used to compose the names of the resource group, application, and application monitor in the automation policy.

  The resource names will appear in the resource table on the operations console. The prefix can be changed. Use no more than a total of 28 alphanumeric characters and underscores. Do not use a leading numeric. Reserved words are not allowed (see the “List of Reserved Words” in the HACMP Administration Guide, SC23-4862.).

  Note that if the HACMP adapter policy has been defined using the current prefix, you must remove this policy before changing the prefix.

  For more information about defining the adapter automation policy, refer to “Defining the HACMP adapter automation policy” on page 193.

Service IP label
  The Service IP label is an entry in /etc/hosts that represents a service IP label. It must be different from the host name of any node in the HACMP cluster. It should be requested from the network administrator as a "service IP label" or "alias" for all nodes in the HACMP cluster and must have been created (for example, using the SMIT interface) before you invoke the configuration dialog.

  The HACMP adapter will listen on the service IP label for requests from the host using the adapter, regardless on which node it runs.

Security tab
The security tab lets you configure the security for the interface between the HACMP adapter and the end-to-end automation management host.

**Fields and controls on the Security tab:**

Select the Enable SSL check box if you want to use the Secure Socket layer (SSL) protocol. If checked, the following entry fields must be completed.

- **Truststore** Name of the truststore file used for SSL. The file name may contain multiple period characters. Click **Browse** to select a file.
- **Keystore** Name of the keystore file used for SSL. The file name may contain multiple period characters. Click **Browse** to select a file.
- **Keystore password** Password of the keystore file. The password is required if a keystore file was specified. Click **Change** to change the password.
  
  **Note:** If the truststore is in different file than keystore, the passwords for the files must be identical.
- **Keystore alias** Alias name of the certificate to be used by the server. If not specified, the keystore file must contain only one entry which is the one to be used.

The Enforce user authentication check box enables user authentication with the Pluggable Access Module (PAM). This check box is selected by default. It should only be deselected for test purposes when user authentication is not required.

- **PAM Service** The name of an entry in file /etc/pam.conf that determines which
check are made to authenticate a user. The default value is su, which checks users as if they were trying to execute the command su.

**Logger tab**
Use the Logger tab to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the configuration file.

![Automation Adapter Configuration](image)

*Figure 24. HACMP configuration dialog: Logger tab*

On the Logger tab, you can perform the following tasks:

**Change the settings permanently**
Perform these steps:
1. Make the required changes on the tab.
2. Click **Save**.

**Results:**
The settings in the configuration file are updated. You must restart the adapter for the changes to take effect.

**Change the settings temporarily**
Perform these steps:
1. Make the required changes on the tab.
2. Click **Apply**.
**Results:**
The new settings take effect immediately. They are not stored in the configuration file. If the adapter is not running, you receive an error message.

**Revert to the permanent settings**
If you changed the settings temporarily, perform the following steps to revert to the permanent settings defined in the configuration file, or when you are unsure which settings are currently active for the adapter:
1. Invoke the configuration dialog and open the Logger tab. The Logger tab displays the values that are currently set in the configuration file.
2. Click **Apply** to activate the settings.

**Results:**
The settings take effect immediately. If the adapter is not running, you receive an error message.

**Controls and fields on the Logger tab:**

- **Maximum log/trace file size**
  - The maximum file size in kilobytes that each log file can reach before it rolls over.

- **Message logging level:**
  - Error: Logs messages on the error level.
  - Warning: Logs messages on the error and warning levels.
  - Information: Logs messages on the error, warning, and informational levels.

- **Trace logging level:**
  - Off: Collects no trace information. (Not recommended.)
  - Minimum: Collects trace information on the error level. Only severe error situations are traced. This is the default setting.
  - Medium: Collects trace information on the error and warning levels.
  - Maximum: Provides the message and trace logs and collects additional information on the error, warning, and informational level. Required for testing and problem determination.

- **First failure data capture (FFDC) settings:**
  - Recording level:
    - Off: Collects no FFDC information.
    - Minimum: Provides the message and trace logs and collects additional information on the error level.
    - Medium: Provides the message and trace logs and collects additional information on the error and warning level.
    - Maximum: Provides the message and trace logs and collects additional information on the error, warning, and informational level.

- **Disk space:**
Maximum disk space
Specifies the maximum disk space in bytes used by FFDC traces which are written to the FFDC trace directory. The default space is 10485760 byte (10MB).

Space exceeded policy
Select what to do if the maximum disk space is exceeded:

Ignore  Issue warnings, but do not enforce the FFDC disk space quota.

Auto-delete
Automatically delete FFDC files, oldest first, until the directory is below the limit. This is the default setting.

Suspend
Halt further FFDC actions until the directory is manually cleaned up.

• Message IDs:

Filter mode  Initiates the tracing of FFDC data depending on the message IDs listed in Message ID list.

Message ID list
Specifies the message IDs that are to trigger tracing, depending on the filter mode. Wildcards, for example, *E (for all error messages), are allowed.

Saving the configuration
Click Save on the configuration dialog to save your changes to the adapter configuration files. Upon completion, the Configuration update status panel appears, showing the list of configuration files that were updated.

Notes:
1. If the service IP label specified on the Automation tab does not match the host specified on the Adapter tab, you are prompted for input. On the panel that appears, click the button Adapter automation.
2. When entries are missing or a value you have entered is out of range (for example, a port number), an error message is displayed.
3. If you made changes on the Automation tab, a message appears reminding you to launch the Define automation policy task.
4. If not noted otherwise, you must restart the adapter for the changes to become effective.
Replicating the HACMP adapter configuration files to other nodes in the domain

After configuring an HACMP adapter on a node, you use the Replicate function to propagate the changes to the other nodes in the HACMP cluster. To use the Replicate function, go to the main panel of the configuration dialog and click Replicate. The Replicate configuration files panel is displayed:

Use this window to distribute (replicate) the HACMP adapter configuration itself or configuration updates to the remaining nodes in the HACMP cluster:

1. Select the configuration files you want to replicate or click Select all to select all configuration files in the list.
2. If the user ID and password you specified are valid on all nodes, you can click Select all below the list of replication target nodes. This ensures that the adapter configuration is identical on all nodes.
3. Enter the user ID and password for the target nodes you want to replicate the files to.
4. Start the replication by clicking Replicate.
Replication may take a while. While the files are being replicated, the Replicate button is indented and grayed-out. When the replication is complete, the replication status of each configuration file is displayed.

**Defining the HACMP adapter automation policy**

If definitions for the automation of the HACMP adapter have been made, clicking Define on the main panel of the configuration dialog will create the resources with the resource name (Resource-/group prefix) as described on page 187. Note that if automated resources with the same name already exist, they are removed before the new resources are created.

If you used the default resource name prefix, the following resources will be defined or queried:

<table>
<thead>
<tr>
<th>Resource class</th>
<th>Resource name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM.HacmpResourceGroup</td>
<td>hacadapter_rg</td>
<td>The resource group that comprises all automated resources.</td>
</tr>
<tr>
<td>IBM.HacmpApplication</td>
<td>hacadapter</td>
<td>Commands: hacadapter start, hacadapter stop</td>
</tr>
<tr>
<td>IBM.HacmpAppMonitor</td>
<td>hacadapter_mon</td>
<td>Command: hacstatus</td>
</tr>
<tr>
<td>IBM.HacmpServiceIP</td>
<td>&lt;service_ip_label&gt; value</td>
<td>The label of the service IP on which the host using the adapter accesses the adapter. This value is not defined but just queried and, therefore, not removed.</td>
</tr>
</tbody>
</table>

When you click Define, the button may stay indented for minutes until the resources have been removed, the cluster is synchronized, the new resources are created, and the cluster is synchronized again. The dialog will not repaint after it has been covered and uncovered. Eventually, the results of the commands are displayed in a pop-up window.

**Removing the HACMP adapter automation policy**

You typically use the Remove function before you change the name prefix of the automated resources (see page 187). When the adapter is automated and you deselect the check box Automate adapter in system automation domain on the Automation tab, you receive a message reminding you to remove the automated resources for the adapter.

Clicking Remove on the main panel of the configuration dialog will remove the resources shown in Table 64. If the HACMP adapter is still running, it is stopped before the automated resources are removed.

When you click Remove, the button may stay indented for minutes until resources have been removed and the cluster has been synchronized. Eventually, the results of the commands are displayed in a pop-up window.
Verifying the HACMP adapter configuration

You can use the clstat command to verify that the HACMP adapter is running:

1. Open a terminal session on the nodes on which the HACMP adapter may run.
2. In each session, type /usr/es/sbin/cluster/clstat
3. The status screen depicted below should be displayed:

   - Resource Group: hacadapter_rg (if the prefix is ‘hacadapter’) in State: Online
   - Interface: p57067ha (in the example configuration) associated with the service IP label of the same name in State: UP

```
clstat - HACMP Cluster Status Monitor
-------------------------------------
Cluster: hacp57067 (1137142142)
Mon Feb 20 14:15:16 MET 2006
  State: UP   Nodes: 2
  SubState: STABLE

   Node: p570sa06   State: UP
     Interface: p570sa06 (0)   Address: 9.152.20.176
     State: UP
     Interface: p57067ha (0)   Address: 9.152.24.195
     State: UP
   Resource Group: hacadapter_rg   State: Online

   Node: p570sa07   State: UP
     Interface: p570sa07 (0)   Address: 9.152.20.177
     State: UP
```

Controlling the HACMP adapter

You use the hacadapter command to start, stop, and monitor the adapter.

*Table 65. HACMP adapter command options*

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hacadapter status</td>
<td>Checks if the adapter is running and returns the RSCT return code for its operational state (OpState):</td>
</tr>
<tr>
<td>0</td>
<td>Unknown. The adapter status cannot be determined.</td>
</tr>
<tr>
<td>1</td>
<td>Online. The adapter is running.</td>
</tr>
<tr>
<td>2</td>
<td>Offline. The adapter is not running.</td>
</tr>
<tr>
<td>hacadapter start</td>
<td>Starts the adapter if it is not running:</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is automated, the command requests HACMP cluster services to start the adapter on the preferred node. The command returns when the clRGmove command completed.</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is not automated, it is started on the node where the command was issued. The exit code is 0 if the command was successful.</td>
</tr>
</tbody>
</table>
Table 65. HACMP adapter command options (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| hacadapter stop | Stops the adapter if it is running:  
|             | • If the adapter is automated, the command requests HACMP cluster services to stop the adapter on the node where it is currently active. The command returns when the `clRGMove` command completed.  
|             | • If the adapter is not automated, it is stopped on the node where the command was issued. The exit code is 0 if the command was successful. |
Chapter 20. Installing and configuring the MSCS adapter

The following topics describe how to install and configure the MSCS adapter.

**Installation and configuration roadmaps**

Before you install the MSCS adapter, you must decide whether you want to make the adapter highly available, which is strongly recommended. The roadmaps provided in this section give an overview of the steps you need to perform to install and configure the adapter depending on your high-availability decision.

**Roadmap for highly available adapters**

If you are making your adapter highly available, which is highly recommended, perform the following steps:

1. Plan and prepare for the installation and configuration of the MSCS adapters (see “Planning and preparing for the MSCS adapter” on page 198).

2. Use the installation wizard to install the adapter on one node in the cluster and generate a response file (see “Using the installation wizard to install the MSCS adapter” on page 199).

3. To ensure that uniform installation parameters are used, use the response file to install the adapters on the remaining nodes. Response-file driven installation can be performed in silent mode (see “Installing the adapter in silent mode” on page 201) or in interactive mode using the installation wizard (see “Using the installation wizard to install the MSCS adapter” on page 199).

4. Configure the adapter on one of the cluster nodes using the adapter configuration dialog (see “Configuring the MSCS adapter” on page 201).

5. To ensure that uniform configuration parameters are used, replicate the adapter configuration files to the remaining nodes (see “Replicating the configuration files to other nodes” on page 209).

6. Create the MSCS resources needed for making the adapter highly available.

7. Verify the installation and configuration (see “Verifying the installation and configuration” on page 216).

**Roadmap for adapters that are not highly available**

If you are not making your adapter highly available, perform the following steps:

1. Plan and prepare for the installation and configuration of the MSCS adapter (see “Planning and preparing for the MSCS adapter” on page 198).

2. Use the installation wizard to install the adapter on a cluster node (see “Using the installation wizard to install the MSCS adapter” on page 199).
3. Configure the adapter using the adapter configuration dialog (see "Configuring the MSCS adapter" on page 201).

4. Verify the installation and configuration (see "Verifying the installation and configuration" on page 216).

Planning and preparing for the MSCS adapter

Packaging

The MSCS adapter is shipped with the End-to-End Automation Management component. This is where you find the installation file:

- **CD:**
  
  You install the adapter from the CD "Tivoli System Automation for Multiplatforms - End-to-End component, Automation Adapters all platforms". This is where you find the installation wizard file (setup.exe) on the CD:  
  EEZ2300Adapters\EEZ2300MSCS\Windows\setup.exe

- **Electronic distribution:**
  
  If you obtain the End-to-End Automation Management component through electronic distribution, you use the following archive to install the MSCS adapter:  
  C106EML.exe
  
  To extract the archive, run the executable. The resulting directory structure is identical to that on the CD. This is where you find the installation wizard file (setup.exe) when you have extracted the archive:  
  EEZ2300Adapters\EEZ2300MSCS\Windows\setup.exe

Installation prerequisites

Note that the MSCS adapter can only be connected to an End-to-End Automation Management component V2R2 or later.

The system on which you are installing the adapter must meet the following installation prerequisites:

- Windows Server 2003 Enterprise Edition with Service Pack 1 or later
- 32-bit systems only
- System must be an MSCS node
- System must not be a domain controller, or local user IDs must be permitted on the domain controller
- 64 MB RAM is required for running the MSCS adapter service
- 40 MB RAM is required for running the adapter configuration dialog
- Disk space requirements:
  - 140 MB for MSCS adapter installation
  - Typically, 6 MB is sufficient during normal operation, however, up to 250 MB may be required for service-related files in the Tivoli Common Directory (log files, FFDC files)
Planning and preparing for high availability

Making the MSCS adapter highly available using MSCS is highly recommended but not required. To prepare for making an adapter highly available, do this:

- Obtain a virtual IP address:
  - The MSCS adapter will use this IP address for incoming connections
  - MSCS will make the virtual IP address available on the appropriate MSCS node
- If desired, obtain a network name:
  - If you specify the network name in the MSCS adapter configuration, the name will be published to the end-to-end automation server
  - The end-to-end automation server will use this network name for connecting to the MSCS adapter
  - MSCS will associate this network name with the virtual IP address on the DNS server that is configured in the Microsoft Windows domain

Installation directories

For the MSCS adapter installation directory and the Tivoli Common Directory, the following restrictions apply:

- The MSCS adapter installation directory name must not include the DBCS space character. The SBCS space character is supported.
- Tivoli Common Directory:
  When specifying a directory other than the default, observe the following restrictions:
  - The directory name has to consist of the platform-specific path separator character and alphanumeric characters (A..Z, a..z, 0..9).
  - The colon character is allowed only once, immediately following the drive letter. For example, C:\<directory_name> is allowed, but C:\<directory_name>:<directory_name> is not allowed.
  - The space character and the underscore character (_) are allowed.

Installing the MSCS adapter

You have the following options to install an MSCS adapter:

- You use the installation wizard to install the adapter.
- You generate a response file when you use the installation wizard on a node.
You can then use the response file in one of two ways to install the adapter on other nodes:
  - You launch the installation wizard using the response file as input. The values in the response file will appear in the fields on the wizard panels and can be changed.
  - You can install the adapter in silent mode on the remaining nodes of the cluster if you are making the adapter highly available, in which case the values in the response file apply to all nodes.

Using the installation wizard to install the MSCS adapter

This section describes how you install the MSCS adapter using the installation wizard. For information on silent mode, see “Installing the adapter in silent mode” on page 201.
**Note:** The MSCS adapter requires the Windows service JaasLogon. JaasLogon is part of the IBM Java Runtime Environment, which is installed during adapter installation. If the service is already installed on the system, it will be replaced during adapter installation.

Perform the following steps to install the adapter:

1. Log in as a local user. The user ID must have administrator privileges. Note that installation will be denied if you are logged in with a domain user ID.

2. Launch the installation wizard. You have the following options:
   - To launch the installation wizard without generating a response file, use the file:
     ```
     setup.exe
     ```
     When you launch the wizard in this way, the values that are displayed on the wizard panels are either default values or values that were detected on your system.
   - To launch the installation wizard, generating a response file, use the following command:
     ```
     setup.exe -DprepareSilent=true
     ```
     This is the response file that is generated:
     ```
     <install_root>/install/install.properties
     ```
     When you launch the wizard in this way, the values that are displayed on the wizard panels are either default values or values that were detected on your system.
     When you have launched the wizard, click **Next** on the Welcome panel to display the license agreement.

3. Select **I accept both the IBM and the non-IBM terms**, to agree to the license agreement. Click **Next**. The Installation directory panel is displayed.

4. Specify the directory where you want to install the adapter or accept the default location. Click **Next** to display the Tivoli Common Directory panel.

5. If the installation program did not detect a Tivoli Common Directory on your system, accept the default location or specify a different directory. If a Tivoli Common Directory was detected on your system, the directory is displayed and cannot be changed.
   Click **Next** to display the Microsoft Cluster Adapter service user panel.

6. The user ID is retrieved from the Windows registry. If the entry field is empty, no valid user ID was found. This indicates that the node where the installation is performed is not a member of a MSCS cluster
   Click **Next** to display the summary panel.

7. Check the values on the summary panel and click **Install** to start the installation.

8. While the adapter is being installed, a progress panel is displayed.
When the installation is complete, an installation summary panel is displayed, on which you can verify the success of the installation. If problems occur, check the applicable installation log files for more information. Click Finish to close the installation wizard.

---

**Installing the adapter in silent mode**

This section describes how you install the adapter in silent mode, using a response file you generated during wizard-driven installation. For information on how to generate a response file and how to use it as input for a wizard-driven installation, see “Using the installation wizard to install the MSCS adapter” on page 199.

To install the MSCS adapter in silent mode, use the following command:

```bash
setup.exe -i silent -f <response_file_name>
```

**Notes:**

1. Response files contain password information and should be deleted when they are no longer needed.
2. The silent installation will only be successful if the wizard-driven installation where the response file was generated completed successfully without errors.

---

### Configuring the MSCS adapter

You use the adapter configuration dialog to configure your MSCS adapter. If your MSCS adapter is highly available, you always configure the adapter on one node and replicate the configuration file to the remaining cluster nodes as described in “Replicating the configuration files to other nodes” on page 209.

You have two configuration alternatives which are mutually exclusive:

- **You can configure the adapter for the operations console of the Base component of IBM Tivoli System Automation.** In this case, the adapter is accessed directly by the operations console, without communicating via the end-to-end automation manager. This operations console mode is referred to as *direct access mode*.

- **If the End-to-End Automation Management component is installed, you can configure the adapter for end-to-end automation management.** This is required if you want to implement end-to-end automation and run the operations console in end-to-end automation mode, or if you want to use the operations console of the End-to-End Automation Management component in first-level automation mode. (For more information on end-to-end automation management and these console modes, refer to the [IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator’s and User’s Guide](https://www.ibm.com).)

---

### Invoking the MSCS adapter configuration dialog

To invoke the configuration dialog, issue the following command:

```bat
cfgmscsadapter.bat
```

The file is located in the adapter installation directory, in the subdirectory bin. The default directory is

```
C:\Program Files\IBM\tsamp\eez\mscs\bin
```

The main panel of the configuration dialog is displayed:
The dialog lets you perform the following tasks:
1. Configure the MSCS adapter.
2. Replicate the MSCS adapter configuration files to other nodes.
3. Define the MSCS adapter automation policy to create the resources required to automate the adapter.
4. Remove the MSCS adapter automation policy.

**Configuring the MSCS adapter**

On the main panel of the configuration dialog, click **Configure** to display the configuration tabs that are described in the following sections.

In the following description, the term **Host using the adapter** is used to refer to either the end-to-end automation manager or the Base component operations console.

**Adapter tab**

On the Adapter tab, you can configure the adapter host.
Fields and controls on the Adapter tab:

Automation adapter host:

Host name or IP address
- If the MSCS adapter is highly available, specify the network name or IP address you obtained as described in “Planning and preparing for high availability” on page 199.
- If the MSCS adapter is not highly available, specify the IP address or host name of the system on which the adapter is running.

Request port number
Specify the number of the port on which the adapter listens for events from host using the adapter. The default port is 2001.

Automation domain

The domain name is the name by which the Microsoft Server Clustering (MSCS) cluster is known to the host using the adapter. The domain name must be unique within the scope of automation domains that connect to an end-to-end automation manager or SA operations console.

You have the following options to specify the domain name:
- It is recommended that you use the MSCS cluster name as domain name. This option is selected by default. You must keep this setting if you want to use Tivoli Enterprise Portal launch-in-context support, which allows you to launch Tivoli Enterprise Portal work spaces from the SA operations console, because Tivoli Enterprise Portal will not recognize any other domain name.
If you cannot use the MSCS cluster name as domain name, for example, because it would not be unique, you can specify a domain name for the Microsoft Server Clustering (MSCS) cluster.

Clicking Advanced lets you specify the adapter runtime behavior:

**Adapter stop delay**

The number of seconds by which the adapter stop is delayed to allow the adapter to properly deliver the domain leave event. The default value is 5. You may need to increase the value on slow systems. Valid values are 3 through 60.

**Remote contact activity interval**

The time period, in seconds, after which the adapter will stop if it was not contacted by the **host using the adapter**, which periodically contacts the adapter to check if it is still running. The default value is 360. If a value other than 0 is specified, the interval must be a multiple of the check interval.

When the value is set to 0, the adapter continuously runs and never stops. This is the recommended setting for adapters that are connected to a Base component operations console, because otherwise the adapter will be stopped whenever the operations console is stopped.

**Initial contact retry interval**

The time period, in minutes, within which the adapter will attempt to contact the **host using the adapter** until it succeeds or the specified time has elapsed. The default value is 0, which means that the adapter will attempt to contact the **host using the adapter** indefinitely.

**EIF reconnect attempt interval**

The time period, in seconds, that the adapter will wait before it attempts to reestablish the connection to the **host using the adapter** after the connection was interrupted. The default value is 30.

**Host using adapter tab**

Use the Host using adapter tab to determine which host the adapter connects to and to specify the required information.

The MSCS can be configured to connect to one of these host:

- An end-to-end automation management host
- A Base component operations console, which runs in direct-access mode

An adapter can only connect to a single host, the configurations are mutually exclusive.
Fields and controls on the Host using adapter tab:

Configure end-to-end automation management host:

Host name or IP address
The name or IP address of the host on which the end-to-end automation manager runs. The port number specified here must match the port number specified as event port number when configuring the domain of the end-to-end automation manager.

Event port number
The port on which the end-to-end automation manager listens for events from the MSCS adapter. The default port is 2002.

Configure direct access operations console:

Host name or IP address
The name or IP address of the host on which the operations console runs.

Event port number
The port on which the operations console listens for events from the MSCS adapter. The default port is 2002.

Security tab
Use the Security tab to configure security for the interface between the MSCS adapter and the end-to-end automation management host.
Select the **Enable SSL** check box if you want to use the Secure Socket layer (SSL) protocol. If checked, the following fields must be completed:

- **Truststore**: Name of the truststore file used for SSL. The file name may contain multiple period characters. Click **Browse** to select a file.

- **Keystore**: Name of the keystore file used for SSL. The file name may contain multiple period characters. Click **Browse** to select a file.

- **Keystore password**: Password of the keystore file. It is required if a keystore file was specified. Click **Change** to change the password.

  **Note**: If the truststore is in different file than keystore, the passwords for the files must be identical.

- **Keystore alias**: Alias name of the certificate to be used by the server. If not specified, the keystore file must contain only one entry which is the one to be used.

**User authentication**

It is recommended that you select the corresponding check box to enforce authentication of the user ID on behalf of which the **host using the adapter** requests operations from the MSCS adapter.

**Logger tab**

Use the Logger tab to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the configuration file.
On the Logger tab, you can perform the following tasks:

**Change the settings permanently**

Perform these steps:
1. Make the required changes on the tab.
2. Click **Save**.

**Results:**
The settings in the configuration file are updated. You must restart the adapter for the changes to take effect.

**Change the settings temporarily**

Perform these steps after ensuring that the adapter is running:
1. Make the required changes on the tab.
2. Click **Apply**.

**Results:**
The new settings take effect immediately. They are not stored in the configuration file. If the adapter was not running, you receive an error message.

**Revert to the permanent settings**

If you changed the settings temporarily, perform the following steps to revert to the permanent settings defined in the configuration file, or when you are unsure which settings are currently active for the adapter:
1. Invoke the configuration dialog and open the Logger tab. The Logger tab displays the values that are currently set in the configuration file.
2. Click **Apply** to activate the settings.

**Results:**
The settings take effect immediately. If the adapter is not running, you receive an error message.
Controls and fields on the Logger tab:

Maximum log/trace file size
   The file size in kilobytes.

Message logging level:
Error       Logs messages on the error level.
Warning     Logs messages on the error and warning levels.
Information Logs messages on the error, warning and informational levels.

Trace logging level:
Off         Collects no trace information.
Minimum     Collects trace information on the error level.
Medium      Collects trace information on the error and warning levels.
Maximum     Provides the message and trace logs and collects additional information on the error, warning, and informational level.

First failure data capture (FFDC) settings:

• Recording level:
  Off         Collects no FFDC information.
  Minimum     Provides the message and trace logs and collects additional information on the error level.
  Medium      Provides the message and trace logs and collects additional information on the error and warning level.
  Maximum     Provides the message and trace logs and collects additional information on the error, warning, and informational level.

• Disk space:
  Maximum disk space
      Specifies the maximum disk space in bytes used by FFDC traces which are written into the FFDC trace directory. The default space is 10485760 byte (10MB).

Space exceeded policy
      Select what to do if the maximum disk space is exceeded.

• Message IDs:
  Filter mode   Initiates the tracing of FFDC data depending on the message IDs listed in Message ID list.
  Message ID list: Specifies the message IDs which trigger the tracing of the FFDC data. Wildcards like *E, meaning all error messages, are allowed.

Saving the configuration
Click Save to save your settings to the adapter configuration files. Upon completion, the configuration update status panel appears, showing the list of configuration files that were updated.

Notes:
1. When entries are missing or a value you have entered is out of range (for example, a port number), an error message is displayed.
2. If not noted otherwise, you must restart the adapter for the changes to become effective.

![Configuration Update Status](image)

**Replicating the configuration files to other nodes**

If your MSCS adapter is highly available, you must replicate the configuration files to the other cluster nodes.

Open the main panel of the adapter configuration dialog and click Replicate. The following window is displayed:

![Replicate Configuration Files](image)

Use this window to distribute (replicate) the MSCS adapter configuration itself or configuration updates to other nodes in the RSCT cluster:

1. Select the configuration files you want to replicate, or click Select all below the configuration file list to select all files in the list.
2. Click Select all below the list of replication target nodes. This ensures that the adapter configuration is identical on all nodes.
3. In the Target node login section, specify a local or domain user ID that is valid on all target nodes. For a local user ID, the specified password must be valid on all target nodes. Domain user IDs must be specified in the form `<user_ID>@<domain_name>`.
4. Click Replicate to start the replication.

Replication may take a while. While the files are being replicated, the Replicate button is indented and grayed-out. When the replication is complete, the replication status of each configuration file is displayed.

![Configuration Update Status](image)
Providing high availability for the MSCS adapter

Perform the following steps:

1. Open the Microsoft Cluster Administrator. Launch the Cluster Application Wizard from the File menu. On the Welcome panel, click Next. The following panels displays:

2. It is recommended that you select Create a new virtual server to create or assign dedicated resources to the MSCS adapter service resources, for example, the virtual IP address.

   Click Next. The following panel is displayed:
3. Define a new group or identify an existing group representing the MSCS adapter as virtual server. In the following steps, this group is referred to as "virtual server group". You should choose the group containing the quorum resource. If you choose a different group, this group should only contain resources for making the MSCS adapter service highly available.

   Click Next. The Resource Group Name panel is displayed:

### Resource Group Name

Name the resource group for this virtual server.

- **Name:** MSCS Adapter Group
- **Description:** MSCS group for making the MSCS Adapter service highly available.
4. On the Resource Group Name panel, specify a group name and a description. Click Next. The Virtual Server Access Information panel is displayed:

5. On the Virtual Server Access Information panel, specify a valid new network name under which the MSCS adapter will be reachable. It must be ensured that the operations console or automation manager to which the MSCS adapter will connect is able to resolve this network name.
   If you do not want to use a network name for the MSCS adapter, specify a dummy name and remove it later.
   Specify a valid IP address on which the MSCS adapter can be reached. It must be ensured that the operations console or automation manager to which the MSCS adapter will connect is able to reach the virtual IP address.
   Do not specify the IP address shown in the screen capture because it belongs to the private IP address space.
   If the MSCS adapter is highly available, specify the network name or IP address you obtained as described in "Planning and preparing for high availability" on page 199.
   Click Next to display the Advanced Properties panel:
6. Click **Advanced Properties** to view or modify the properties of the selected MSCS group or resource. Typically the default settings are appropriate but should be checked for correctness and completeness.
   Click **Next** to continue.

7. On the Create Application Cluster Resource panel, select to create a cluster resource for your application now.
   Click **Next** to continue.

8. On the Application Resource Panel, select **Generic Service** from the drop-down list. An MSCS resource of type Generic Service is used to make the service highly available, because the MSCS adapter runs as Windows service.
   Click **Next** to display the following panel:
9. Specify an adapter name and a description.

10. Click Advanced Properties and open the Dependencies page.
11. On the Dependencies page, do this:
   - If you do not want to define a network name for the MSCS adapter, add a dependency on the “IP Address” resource.
   - If you want to define a network name for the MSCS adapter, add a dependency on the “Network Name” resource.

12. Display the Generic Service Parameters panel, type the service name “SA MP MSCS Adapter” in the Service name field. Leave the Start parameters field empty and click Next.

13. On the Registry Replication panel that displays, no entries are required. Click Next.

14. On the completion panel, verify that the configuration settings are correct, and click Finish to save the configuration.

15. If you do not want to use a network name for the MSCS adapter, you can delete it now using the Cluster Administrator:
Verifying the installation and configuration

Perform the following steps to verify that the adapter is installed and configured correctly:

The adapter is highly available:
1. Start the MSCS adapter using MSCS and check if the domain joins.
2. Fail the adapter over to all MSCS nodes and check if the domain joins.

The adapter is not highly available:
- Start the MSCS adapter using the Services plug-in from the Microsoft Management Console and check if the domain joins.

Uninstalling the MSCS adapter

Perform the following steps:
1. Make sure that the MSCS adapter service is stopped before starting the uninstallation.
   Note that MSCS may try to restart or fail the MSCS adapter service over to another MSCS node if you stop the service manually.
   If the MSCS adapter service is highly available, you must take the MSCS adapter group offline.

2. Open the Windows Control Panel and use Add or Remove Programs to uninstall the adapter.
Chapter 21. Installing and configuring the VERITAS Cluster Server adapter

The following topics describe how to install and configure the VERITAS Cluster Server adapter (VCS adapter) on Solaris/SPARC.

Installing the VCS adapter

Packaging

The VCS adapter is shipped with the End-to-End Automation Management component. The name of the binary file you use for installing the adapter is install.bin. This is where you find the installation package:

- **CD:**
  You install the adapter from the CD "Tivoli System Automation for Multiplatforms - End-to-End component, Automation Adapters all platforms". The installation package is available in the installation source directory EEZ2300Adapters/EEZEEZ2300VCS/Solaris.
- **Electronic distribution:**
  If you obtain the End-to-End Automation Management component through electronic distribution, you use the following archive to install the VCS adapter:
  - Deliverable name: C106GML.bin
  - Installation source directory: EEZ2300Adapters/EEZ2300VCS/Solaris

Installation prerequisites

Note that the VCS adapter can only be connected to an End-to-End Automation Management component V2R3 or later.

The system on which you are installing the adapter must meet the following installation prerequisites:

- Solaris 10 on RISC processors
- 64 MB of free RAM
- Minimum color depth: 8-bit (256 colors)
- Minimum screen resolution: 640 x 480

Using the installation wizard to install the VCS adapter

You use an installation wizard to install the VCS adapter on Solaris/SPARC systems.

Perform the following steps:
1. Log in as root on the system where you want to install the VCS adapter.

2. Launch the installation wizard using the file install.bin. On the panel that appears, click **OK** to display the license agreement. The language is detected automatically or you can select it on the first panel.

3. Select **I accept both the IBM and the non-IBM terms** to agree to the license agreement. Click **Next**. The Introduction panel is displayed.
After installing the adapter it must be configured as described in the remaining sections of this chapter.

**Automating the VCS adapter**

If the VCS Solaris/SPARC cluster consists of more than one node, the VCS adapter must be automated for the following reasons:

- The host using the adapter must be able to reach the adapter always through the same service IP without reconfiguration.
- If the node on which the adapter runs goes down or the VCS cluster services on that node are stopped, the adapter must move to another available node in the cluster to resume the connection with the host using the adapter.

For more information about automating VCS adapters using the adapter configuration dialog, see "Automation tab" on page 224.

**Configuring the VCS adapter**

The following figure shows in which environments the VCS adapter can work and what needs to be configured for the adapter.
Figure 28 shows that you have two adapter configuration alternatives which are mutually exclusive:

- You can configure the adapter for the operations console of the Base component of IBM Tivoli System Automation. In this case, the adapter is accessed directly by the operations console, without communicating via the end-to-end automation manager. This operations console mode is referred to as direct access mode.

- If the End-to-End Automation Management component is installed, you can configure the adapter for end-to-end automation management. This is required if you want to implement end-to-end automation and run the operations console in end-to-end automation mode or if you want to use the operations console in first-level automation mode. For more information on end-to-end automation management and these console modes, refer to the IBM Tivoli System Automation for Multiplatforms End-to-End Automation Management Component Administrator's and User's Guide.
Invoking the VCS adapter configuration dialog

The VCS adapter can be configured with the `cfgvcsadapter` utility.

Notes:
1. The `cfgvcsadapter` utility is an X-application and must be used from a workstation with Xserver capabilities. This can be one of your cluster nodes if the X11 optional feature is installed on that node.
2. The 32-bit version of Java 1.4 or Java 5 SR5 must be installed.
3. SSL/SSH packages must be installed and the sshd subsystem must be running to be able to complete the Replication task of the adapter configuration.
4. To use the VCS adapter configuration dialog, you must either be logged in on the system with the user ID root or have write access to the directory `/etc/opt/IBM/tsamp/eez/vcs/cfg`.

To open the configuration dialog, issue the command `cfgvcsadapter`.

The main panel of the dialog is displayed:

![Main panel of the VCS adapter configuration dialog](image)

Figure 29. Main panel of the VCS adapter configuration dialog

The dialog lets you perform the following tasks:
1. Configure the VCS adapter.
2. Replicate the VCS adapter configuration files to other nodes.
3. Define the VCS adapter automation policy to create the resources required to automate the adapter.
4. Remove the VCS adapter automation policy.
Configuring the VCS adapter

On the main panel of the configuration dialog, click Configure to display the configuration tabs that are described in the following sections.
In the following description, the term Host using the adapter is used to refer to either the end-to-end automation manager or the Base component operations console.

Adapter tab
Selecting the adapter tab lets you configure the adapter host.

![Adapter tab of the VCS adapter configuration dialog](image)

Fields and controls on the Adapter tab:

Automation adapter host:

Host name or IP address

Host name or service IP label of the node where the adapter runs.

On initial invocation, the field contains the value the command hostname would return.

If you are automating the adapter, leave the value unchanged. The value will be updated automatically with the value you specify in the field Adapter IP address on the Automation tab (see "Automation tab" on page 224).

Request port number

The port on which the adapter listens for requests from the host using the adapter. The default port is 2001.
Automation domain:

The domain name is the name by which the Microsoft Server Clustering (MSCS) cluster is known to the **host using the adapter**. The domain name must be unique within the scope of automation domains that connect to an end-to-end automation manager or SA operations console.

You have the following options to specify the domain name:

- It is recommended that you use the MSCS cluster name as domain name. This option is selected by default. You must keep this setting if you want to use Tivoli Enterprise Portal launch-in-context support, which allows you to launch Tivoli Enterprise Portal work spaces from the SA operations console, because Tivoli Enterprise Portal will not recognize any other domain name.

- If you cannot use the MSCS cluster name as domain name, for example, because it would not be unique, you can specify a domain name for the Microsoft Server Clustering (MSCS) cluster.

Clicking **Advanced** lets you specify the adapter runtime behavior:

**Adapter stop delay**

The number of seconds by which the adapter stop is delayed to allow the adapter to properly deliver the domain leave event. The default value is 5. You may need to increase the value on slow systems. Valid values are 3 through 60.

**Remote contact activity interval**

The time period, in seconds, after which the adapter will stop if it was not contacted by the **host using the adapter**, which periodically contacts the adapter to check if it is still running. The default value is 360. If a value other than 0 is specified, the interval must be a multiple of the check interval.

When the value is set to 0, the adapter continuously runs and never stops. This is the recommended setting for adapters that are connected to a Base component operations console, because otherwise the adapter will be stopped whenever the operations console is stopped.

**Initial contact retry interval**

The time period, in minutes, within which the adapter will attempt to contact the **host using the adapter** until it succeeds or the specified time has elapsed. The default value is 0, which means that the adapter will attempt to contact the **host using the adapter** indefinitely.

**EIF reconnect attempt interval**

The time period, in seconds, that the adapter will wait before it attempts to reestablish the connection to the **host using the adapter** after the connection was interrupted. The default value is 30.

**Host using adapter tab**

Use the Host using adapter tab to determine which host the adapter connects to and to specify the required information.

The VCS adapter can be configured to connect to one of these host:

- An end-to-end automation management host
- A Base component operations console, which runs in direct-access mode
An adapter can only connect to a single host, the configurations are mutually exclusive.

Figure 31. Host using adapter tab of the VCS configuration dialog

Fields and controls on the Host using adapter tab:

Configure end-to-end automation management host:

Host name or IP address
The name or IP address of the host on which the end-to-end automation manager runs. The port number specified here must match the port number specified as event port number when configuring the domain of the end-to-end automation manager.

Event port number
The port on which the end-to-end automation manager listens for events from the VCS adapter. The default port is 2002.

Configure direct access operations console:

Host name or IP address
The name or service IP label of the host on which the operations console runs.

Event port number
The port on which the operations console listens for events from the VCS adapter. The default port is 2002.
Automation tab

![Automation tab of the VCS configuration dialog](image)

This tab lets you configure the adapter automation policy. This allows you to make the VCS adapter highly available.

**Note:** All nodes where the adapter can run must be accessible using the same user ID and password.

**Fields and controls on the Automation tab:**

Automate adapter in first-level automation domain

Select this check box (see also “Automating the VCS adapter” on page 218).

Query domain If the configuration dialog runs on a node in the VCS cluster, click Query domain to query the current automation policy from the VCS cluster. If the automation policy for the adapter is not yet defined but the cluster is up, at least all nodes that are online are shown in the Defined nodes table. This table provides the following information:

- Defined node
  The list of defined nodes.
- Automate on node
  Indicates if the adapter is automated on this node.

The buttons at the bottom of the table let you perform the following tasks:
• Up
  Moves the selected node one position up in the node sequence. The position determines the order in which automation selects the node on which the adapter may run.

• Down
  Moves the selected node one position down in the node sequence. The position determines the order in which automation selects the node on which the adapter may run.

• Add
  Displays the Add node for adapter automation panel which lets you define the name of the node to be added and determine if the node is to be added to automation of the adapter.

• Remove
  Removes the selected node from the list. This means that the adapter must not be started on that node.

• Change
  Displays the Change node for adapter automation panel which lets you change the name of the node and add or remove the node from automation of the adapter.

Automated resources prefix
The prefix that is used to compose the names of the resource group, application, and application monitor in the automation policy.
The resource names will appear in the resource table on the operations console. The prefix can be changed. It is restricted to ASCII characters; the following characters cannot be used:
" (double quote), ' (single quote), ; (semicolon), $ (dollar), / (slash)
Note that if the VCS adapter policy has been defined using the current prefix, you must remove this policy before changing the prefix.
For more information about defining the adapter automation policy, refer to "Defining the VCS adapter automation policy" on page 231.

Adapter IP address
Regardless on which node it runs, the end-to-end automation adapter uses this address to listen for requests and receive requests from the host using the adapter. You must obtain this IP address from your network administrator. The IP address must neither be an actual host address nor localhost.

Netmask
The netmask that is used in the adapter automation policy. Request a value from your network administrator.

Network interface
The network interface that is used in the adapter automation policy. The adapter can be reached on this network interface through the specified IP address.

Click Query to display the Select network interface dialog, which lets you select one of the network interfaces that are currently defined on the node where the configuration dialog runs.

Note: When you click Save after specifying an IP address in the field Adapter IP address, the following message may be displayed:
The message informs you that the IP addresses on the Adapter and Automation tabs differ and asks you to confirm that the IP address on the Adapter tab is to be updated with the value you specified on the Automation tab. Click Yes to confirm the change.

**Security tab**

![Security tab of the VCS configuration dialog](image)

The security tab lets you configure the security for the interface between the VCS adapter and the end-to-end automation management host.

**Fields and controls on the Security tab:**

Secure Socket Layer (SSL) for transport:

Select the **Enable SSL** check box if you want to use the Secure Socket layer (SSL) protocol. If checked, the following entry fields must be completed.

- **Truststore**
  - Name of the truststore file used for SSL. The file name may contain multiple period characters. Click **Browse** to select a file.
Keystore Name of the keystore file used for SSL. The file name may contain multiple period characters. Click **Browse** to select a file.

Keystore password Password of the keystore file. The password is required if a keystore file was specified. Click **Change** to change the password.

**Note:** If the truststore is in different file than keystore, the passwords for the files must be identical.

Keystore alias Alias name of the certificate to be used by the server. If not specified, the keystore file must contain only one entry which is the one to be used.

User authentication:

It is recommended that you select the corresponding check box to enforce authentication of the user ID on behalf of which the host using the adapter requests operations from the VCS adapter.

**Logger tab**

Use the Logger tab to specify the settings for logging, tracing, and First Failure Data Capture. You can change the settings permanently or temporarily.

Note that the Logger tab always displays the values that are currently set in the configuration file.

---

**Figure 34. VCS configuration dialog: Logger tab**
On the Logger tab, you can perform the following tasks:

**Change the settings permanently**
Perform these steps:
1. Make the required changes on the tab.
2. Click **Save**.

**Results:**
The settings in the configuration file are updated. You must restart the adapter for the changes to take effect.

**Change the settings temporarily**
Perform these steps:
1. Make the required changes on the tab.
2. Click **Apply**.

**Results:**
The new settings take effect immediately. They are not stored in the configuration file. If the adapter is not running, you receive an error message.

**Revert to the permanent settings**
If you changed the settings temporarily, perform the following steps to revert to the permanent settings defined in the configuration file, or when you are unsure which settings are currently active for the adapter:
1. Invoke the configuration dialog and open the Logger tab. The Logger tab displays the values that are currently set in the configuration file.
2. Click **Apply** to activate the settings.

**Results:**
The settings take effect immediately. If the adapter is not running, you receive an error message.

**Controls and fields on the Logger tab:**

**Maximum log/trace file size**
The maximum file size in kilobytes that each log file can reach before it rolls over.

**Message logging level:**
- **Error** Logs messages on the error level.
- **Warning** Logs messages on the error and warning levels.
- **Information** Logs messages on the error, warning and informational levels.

**Trace logging level:**
- **Off** Collects no trace information. (Not recommended.)
- **Minimum** Collects trace information on the error level. Only severe error situations are traced. This is the default setting.
- **Medium** Collects trace information on the error and warning levels.
- **Maximum** Provides the message and trace logs and collects additional information on the error, warning, and informational level. Required for testing and problem determination.

**First failure data capture (FFDC) settings:**
• Recording level:
  Off Collects no FFDC information.
  Minimum Provides the message and trace logs and collects additional information on the error level.
  Medium Provides the message and trace logs and collects additional information on the error and warning level.
  Maximum Provides the message and trace logs and collects additional information on the error, warning, and informational level.

• Disk space:
  Maximum disk space Specifies the maximum disk space in bytes used by FFDC traces which are written to the FFDC trace directory. The default space is 10485760 byte (10MB).

  Space exceeded policy
  Select what to do if the maximum disk space is exceeded:
  Ignore Issue warnings, but do not enforce the FFDC disk space quota.
  Auto-delete Automatically delete FFDC files, oldest first, until the directory is below the limit. This is the default setting.
  Suspend Halt further FFDC actions until the directory is manually cleaned up.

• Message IDs:
  Filter mode Initiates the tracing of FFDC data depending on the message IDs listed in Message ID list.

  Message ID list Specifies the message IDs that are to trigger tracing, depending on the filter mode. Wildcards, for example, *E (for all error messages), are allowed.

**Saving the configuration**
Click Save on the configuration dialog to save your changes to the adapter configuration files. Upon completion, the Configuration update status panel appears, showing the list of configuration files that were updated.

**Notes:**
1. If the Adapter IP address specified on the Automation tab does not match the host specified on the Adapter tab, you are prompted for input. On the panel that appears, click the button **Adapter automation**.
2. When entries are missing or a value you have entered is out of range (for example, a port number), an error message is displayed.
3. If you made changes on the Automation tab, a message appears reminding you to launch the Define automation policy task.
4. If not noted otherwise, you must restart the adapter for the changes to become effective.
Replicating the VCS adapter configuration files to other nodes in the domain

After configuring an VCS adapter on a node, you use the Replicate function to propagate the changes to the other nodes in the VCS cluster. To use the Replicate function, go to the main panel of the configuration dialog and click Replicate. The Replicate configuration files panel is displayed:

1. Select the configuration files you want to replicate or click Select all to select all configuration files in the list.
2. If the user ID and password you specified are valid on all nodes, you can click Select all below the list of replication target nodes. This ensures that the adapter configuration is identical on all nodes.
3. Enter the user ID and password for the target nodes you want to replicate the files to.
4. Start the replication by clicking Replicate.
Replication may take a while. While the files are being replicated, the **Replicate** button is indented and grayed-out. When the replication is complete, the replication status of each configuration file is displayed.

**Defining the VCS adapter automation policy**

If definitions for the automation of the VCS adapter have been made, clicking **Define** on the main panel of the configuration dialog will create the resources with the resource name (Resource-/group prefix) as described on page 225. Note that if automated resources with the same name already exist, they are removed before the new resources are created.

If you used the default resource name prefix, the following resources will be defined or queried:

<table>
<thead>
<tr>
<th>Resource class</th>
<th>Resource name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM.VCS.ResourceGroup</td>
<td>vcsadapter-rg</td>
<td>The resource group that comprises all automated resources</td>
</tr>
<tr>
<td>Application</td>
<td>vcsadapter-rs</td>
<td>Commands: vcsadapter start, vcsadapter stop</td>
</tr>
<tr>
<td>IP</td>
<td>vcsadapter-ip</td>
<td>The virtual IP address on which the host using the adapter accesses the adapter.</td>
</tr>
</tbody>
</table>

When you click **Define**, the button may stay indented for minutes until the resources have been removed, the cluster is synchronized, the new resources are created, and the cluster is synchronized again. The dialog will not repaint after it has been covered and uncovered. Eventually, the results of the commands are displayed in a pop-up window.

**Removing the VCS adapter automation policy**

You typically use the Remove function **before** you change the name prefix of the automated resources (see page 225). When the adapter is automated and you deselect the check box **Automate adapter in system automation domain** on the Automation tab, you receive a message reminding you to remove the automated resources for the adapter.

Clicking **Remove** on the main panel of the configuration dialog will remove the resources shown in [Table 66](#). If the VCS adapter is still running, it is stopped before the automated resources are removed.

When you click **Remove**, the button may stay indented for minutes until resources have been removed and the cluster has been synchronized. Eventually, the results of the commands are displayed in a pop-up window.

**Verifying the VCS adapter configuration**

You can use the **hastatus** command to verify that the VCS adapter is running:

1. Open a terminal session on the nodes on which the VCS adapter may run.
2. In each session, type `/opt/VRTS/bin/hastatus`
3. A status screen similar to the following is displayed, showing the status of the member resources of the resource group `vcsadapter-rg`:  

```
Controlling the VCS adapter

You use the `vcsadapter` command to start, stop, and monitor the adapter.

Table 67. VCS adapter control command options

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcsadapter status</td>
<td>Checks if the adapter is running.</td>
</tr>
<tr>
<td></td>
<td>Available return codes:</td>
</tr>
<tr>
<td></td>
<td>0 Unknown. The adapter status cannot be determined.</td>
</tr>
<tr>
<td></td>
<td>1 Online. The adapter is running.</td>
</tr>
<tr>
<td></td>
<td>2 Offline. The adapter is not running.</td>
</tr>
<tr>
<td>vcsadapter start</td>
<td>Starts the adapter if it is not running:</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is automated, the command requests VCS to start the adapter on the preferred node.</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is not automated, it is started on the node where the command was issued. The exit code is 0 if the command was successful.</td>
</tr>
<tr>
<td>vcsadapter stop</td>
<td>Stops the adapter if it is running:</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is automated, the command requests VCS to stop the adapter on the node where it is currently active.</td>
</tr>
<tr>
<td></td>
<td>• If the adapter is not automated, it is stopped on the node where the command was issued. The exit code is 0 if the command was successful.</td>
</tr>
</tbody>
</table>
Part 5. Appendixes
Appendix A. Preserving user data during the upgrade from IBM Tivoli System Automation 2.2 to IBM Tivoli System Automation 2.3

The upgrade from IBM Tivoli System Automation 2.2.0 to IBM Tivoli System Automation 2.3 requires a migration from WebSphere Application Server 6.0.2 to WebSphere Application Server 6.1, and since the installer technology changes from InstallShield to InstallAnywhere, the upgrade of IBM Tivoli System Automation effectively means that you need to uninstall IBM Tivoli System Automation 2.2 and to install IBM Tivoli System Automation 2.3 as if it were an initial installation. The uninstallation step includes the removal of the automation database (default name: EAUTODB). Among other data, this database contains information about the automation domain topology and the operator preferences.

To preserve the data, you need to export the data before uninstalling IBM Tivoli System Automation 2.2 to be able to import it during the installation of IBM Tivoli System Automation 2.3.

To export the data, perform the following steps before uninstalling IBM Tivoli System Automation 2.2:
1. Stop the WebSphere Application Server to ensure that the automation manager does not lock any data in the database.
2. Change to the “DDL/Script” directory on the product CD and run the following script to export the data:
   **Windows:**
   ```bash
   db2_export_automgr_from_v2200.bat <db_name> <instance_owner> <instance_pwd> <export_to_dir>
   ```
   **AIX, Linux:**
   ```bash
   db2_export_automgr_from_v2200.sh <db_name> <instance_owner> <instance_pwd> <export_to_dir>
   ```
   These are the required parameters:
   - `<db_name>` - Name of the System Automation for Multiplatforms database. Typically, this is EAUTODB.
   - `<instance_owner>` - Database instance owner user id.
   - `<instance_pwd>` - Database instance owner password.
   - `<export_to_dir>` - Absolute path name of the directory where the exported tables should be stored. Ensure that the `<instance_owner>` user ID has write access to this directory.

   All of these parameters are required.
3. Then, uninstall IBM Tivoli System Automation 2.2 and start the installation of IBM Tivoli System Automation 2.3. On the Import Data installation wizard panel, select **Import data to the automation database** and specify the `<export_to_dir>` directory where the exported tables are stored.

**Notes:**
1. Do not use the backup and restore functionality provided by DB2 to backup and restore the automation database, as this preserves the complete database layout.
2. The DB2 export utility that is used by the automation data export script creates several warning messages with message ID SQL3100W. This warning message may be ignored. For further information about this message, refer to the DB2 documentation.
3. Even if the data import step during installation of IBM Tivoli System Automation 2.3 fails, the installation completes. You can check the installation log file, correct the error, and start the import again by using the import scripts provided by the IBM Tivoli System Automation in the same directory as the export scripts listed above. The import scripts have analogous syntax as the export scripts.
Appendix B. Troubleshooting the installation of the Base component operations console

Use this section for troubleshooting problems you experience when installing or configuring the Base component operations console.

Cleaning up from a failed installation

The installation can be canceled at any time. To recover from this situation, just run the installer again.

- Installation was canceled or failed before the installation was started: No cleanup is required.
- Installation was canceled or failed during the installation phase: Run the uninstaller to clean up files that were installed on disk.
- Installation was canceled during the configuration phase: Installation can be resumed.
- Installation failed during the configuration phase: Corrective actions may be needed before installation can be resumed.

If uninstall is desired rather than resume, no unconfiguration is necessary. Uninstall can be immediately called to remove all files from the disk. Uninstall can be run with the option -Dforce=true to be able to proceed even if errors are reported in the pre-uninstall phase.

Procedures for troubleshooting an installation

If the installation fails, the installation wizard displays an error message.

When an error occurs, immediately archive the installation log files (see “Using the log file collector utility” on page 238). This ensures that the original log files are retained, which is important should you need to contact IBM Support, and you can use the archive for your own troubleshooting activities.

An error occurred in the pre-installation phase

If an error occurs in the pre-installation phase, that is, before the Install button was clicked, click the button Save installation log files on the error panel to collect all installation log files. The zip file will be created at the location specified.

An error occurred in the installation phase:

Typically, errors only occur in the installation phase if insufficient disk space is available.

An error occurred in the configuration phase:

Click Finish to finish the installation, then change to <EEZ_INSTALL_ROOT>/install and run the log file collector utility. The log zip will be created in the same directory. For details see “Using the log file collector utility” on page 238.
Known problems

**Attempt to connect to the Base component operations console fails**

**Symptom:** The attempt connect to the Base component operations console fails although it is installed correctly and the embedded version of WebSphere Application Server is running.

**Example:** When you try to open the administrative console by directing your browser to http://<your_host_name>:<port>/admin using the default port number 9060, you receive an error message indicating that the page cannot be opened.

**Explanation:** If any other installation of WebSphere Application Server (including installations of the embedded version) already exists on the system, the installation of the new embedded version automatically increments the port numbers it listens on.

**Solution:** Determine the ports on which the embedded version of WebSphere Application Server that was installed for the Base component operations console is listening. (For example, on Linux, after having started WebSphere Application Server, use the command “netstat -anp | grep java” to retrieve the list of ports that were opened by Java processes). Then direct the browser to the listening port of the administrative console.

**Using the log file collector utility**

When an error occurs, use the you log file collector utility to collect the log files that were written during the installation. The utility generates an archive that you can use for your own troubleshooting activities and send to IBM Support if you cannot resolve the error.

Perform these steps to run the log file collector utility:

1. Change the directory to `<EEZ_INSTALL_ROOT>/install`.
2. Issue the following command:

   **Windows:** `collectinstallerlogs.bat`  
   **AIX/Linux:** `collectinstallerlogs.sh`  

   The command can be invoked with the option `-D` to only copy all logs (in case Java is not available); the directory tree created can then be packed manually.

   Name of the file that is created by the utility:
   `eezinstallerlogs_<timestamp>.zip`  

   On AIX and Linux, you can invoke the command with the option `tar` to use tar rather than jar for packing.

   The resulting archive has the following directory structure:
   - `EEZ_logs`  
   - `cfg`: configuration files (for the automation engine, etc.)  
   - `logs`: `eezinstall.log`, etc.  
   - `sh` / `bat` (Linux/AIX: `sh`; Windows: `bat`): scripts used by installer  
   - `WAS_logs`  
   - `logs`: general WAS server logs  
   - `<server name>`: logs for the selected WebSphere Application Server

**Gathering information for IBM Support**

If you cannot resolve an installation problem, send the installation log file archive to IBM support (see “Using the log file collector utility”).
Appendix C. Troubleshooting the installation of the Base component for Windows

The Base component for Windows does not become operational after installation

For the Base component for Windows to become operational after installation, the Administrator UID must be set correctly. Typically, this is ensured if you have performed the procedures described in “Ensuring that the Administrator UID is set to the correct value” on page 49.

If the UID is not set correctly, perform these steps:
1. Log in using the administrator account you use for operating the Base component for Windows.
2. Open a shell, for example, a Korn shell.
3. Issue the command id to retrieve information about your account. The output of this command should look similar to this example:

   > id
   uid=197108(Administrator) gid=197121(None) groups=197121(None), 5792(+Everyone), 131616(+Administrators), 131617(+Users), 66820(+INTERACTIVE)66827(+Authenticated Users), 66831(+This Organization), 4095(CurrentSession), 66820(+LOCAL), 262154(NT AUTHORITY\NTLM Authentication)

4. Make a make a note of the UID and GID displayed in the output.
5. Create the file /var/ct/cfg/ctadmins.cfg. Add these lines to the file:

   UID=<your_administrator_UID>
   GID=<your_Administrator_GID>

6. Stop all subsystems under the control of the System Resource Controller by issuing stopsrc -a.
7. Stop and re-start the System Resource Controller Windows service
8. Re-start the ctrmc subsystem by issuing rmctctrl -s
9. Make sure that users have the required access rights on the file

   %SystemRoot%/system32/drivers/etc/services:
   • The principal user SYSTEM must have at least read access to the file.
   • The administrator you are using with Tivoli System Automation, this user must have read and write access to the file.

   Sufficient access rights can best be achieved by granting the local or Windows domain Administrator full access to the file.

   To view or change the access rights, you can either use the Windows file explorer or the Windows command cacls. The output of the command will look similar to this example:

   > cacls services C:\WINDOWS\system32\drivers\etc\services NODE2\Administrator:F
   NT AUTHORITY\SYSTEM:R

Manually uninstalling the Base component for Windows

Perform these steps to manually uninstall the Base component for Windows:
1. Remove the program installation folder (typically, this is C:\Program Files\IBM\Tivoli SA MP Base)
2. Remove the RSCT program directory: C:\Windows\SUA\usr\sbin\rsct (change to a different drive, if necessary.)

3. Remove the following registry entries:
   - HKEY_LOCAL_MACHINE\SOFTWARE\IBM\TSA
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Tivoli SA MP Base
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\RSCMM
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\RSCNLV
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SAMMM
   - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SAMNLV

4. To remove everything that was installed, delete the files listed below (change to a different drive, if necessary). Note that the installer just overwrites these files if they are still present at installation time:
   - C:\WINDOWS\SUA\bin\chserver
   - C:\WINDOWS\SUA\bin\chsrcmeth
   - C:\WINDOWS\SUA\bin\chsys
   - C:\WINDOWS\SUA\bin\confsrc
   - C:\WINDOWS\SUA\bin\llsrc
   - C:\WINDOWS\SUA\bin\mknotify
   - C:\WINDOWS\SUA\bin\mkserver
   - C:\WINDOWS\SUA\bin\mksrcmeth
   - C:\WINDOWS\SUA\bin\mkssys
   - C:\WINDOWS\SUA\bin\odcreate
   - C:\WINDOWS\SUA\bin\printenv
   - C:\WINDOWS\SUA\bin\refresh
   - C:\WINDOWS\SUA\bin\rmnotify
   - C:\WINDOWS\SUA\bin\rmserver
   - C:\WINDOWS\SUA\bin\rmsrcmeth
   - C:\WINDOWS\SUA\bin\rmssys
   - C:\WINDOWS\SUA\bin\startsrc
   - C:\WINDOWS\SUA\bin\stopsrc
   - C:\WINDOWS\SUA\bin\tracesoff
   - C:\WINDOWS\SUA\bin\traceson
   - C:\WINDOWS\SUA\bin\winifconfig
   - C:\ WINDOWS\SUA\bin\winsyslocale
   - C:\WINDOWS\SUA\etc\objrepos\SRCextmeth
   - C:\WINDOWS\SUA\etc\objrepos\SRCnotify
   - C:\WINDOWS\SUA\etc\objrepos\SRCsubsvr
   - C:\WINDOWS\SUA\etc\objrepos\SRCsubsys
   - C:\ WINDOWS\SUA\usr\lib\libsrc.so
   - C:\WINDOWS\SUA\usr\lib\libsrcdb.so
   - C:\WINDOWS\SUA\usr\lib\libplatform.so
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\ct_cu.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\ct_mc.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\ct_rm.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\ct_sr.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\dsmsg.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\ffdc.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\configmcli.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\ctccli.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\cerrmcli.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\ffdccat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\mclcli.cat
   - C:\WINDOWS\SUA\usr\lib\nlsmsg\en_US\sccli.cat
   - C:\WINDOWS\SUA\usr\include\rsct\GSClient.h
   - C:\WINDOWS\SUA\usr\include\rsct\GSController.h
   - C:\WINDOWS\SUA\usr\include\rsct\GSObject.h
   - C:\WINDOWS\SUA\usr\include\rsct\GSPublisher.h
   - C:\ WINDOWS\SUA\usr\include\rsct\GSSubscriber.h
5. Remove the **Start** menu entries (typically, this is **Start > Programs > Tivoli SAMMP Base**).
Appendix D. Troubleshooting the installation of the End-to-End Automation Management component

Use this section for troubleshooting problems you experience when installing or configuring the End-to-End Automation Management component.

Installation wizard cannot find WebSphere Application Server on the system

WebSphere Application Server must be installed on the system before end-to-end automation management can be installed. If the installation wizard of Tivoli System Automation for Multiplatforms does not detect WebSphere Application Server on the system but you did install it, the WebSphere Application Server installation may be damaged. You can specify the location manually. If WebSphere Application Server is found it will be used, if possible.

Determining the correct DB2 port number

When you install the End-to-End Automation Management component on AIX or Linux systems, the installation wizard can retrieve the valid DB2 instance port number automatically. If you opt not to use this function, or on Windows systems, the port number 50000 will be displayed in the entry field on the corresponding installation wizard panel, which is the default port number that is assigned to DB2 during the installation of DB2. However, if the port is not free, a different port number is assigned automatically, which is why you need to check if the default port number is correct.

This is how you can determine the correct DB2 port number:

- All operating systems:
  - The port number is displayed in the summary panel that appears when the DB2 installation is complete.
- You can also determine the port number in this way:
  1. Log on as the instance user (for example, db2inst1)
  2. Issue the command `db2 get dbm cfg`
  3. Go to the following line:

     TCP/IP Service name (SCVENAME) = db2c_DB2

    the string after (SCVENAME) = is the DB2 instance port.

    If the string is numeric, for example, 50000, it is the instance port number. If the string is not numeric, for example, db2c_DB2, look for a string similar to `db2c_DB2 50000/tcp` in this file:

    AIX/Linux:
    `/etc/services`

    Windows:
    `C:\WINDOWS\SYSTEM32\DRIVERS\ETC\SERVICES`
DB2 access test hangs

If the attempt to access the database does not return (an indeterminate dialog is shown for a very long time), the test may be hung. The DB2 password may be expired. To resolve the problem, perform these steps:

1. End the installer. Because Cancel is not enabled at this point, you must end the installer using the Task manager (on Windows systems) or the kill command (on UNIX systems). If the installer is killed, files in the system temporary directory remain on the system. If desired, you can manually delete the files in the following way:
   - **AIX/Linux:** Delete the directories /tmp/<xxxxxx>,tmp and /tmp/install.dir.<xxxxxx> (<xxxxxx> stands for an arbitrary number)
   - **Windows:** Delete the directory C:\Documents and Settings\Administrator\Local Settings\temp\Ixxxxxxx (<xxxxxx> stands for an arbitrary number)
2. Check if the DB2 password is expired.
3. Renew the DB2 password.
4. Restart the installation.

Exceptions appear in file eezinstall.log

Any NoClassDefFoundError exceptions that appear in the eezinstall.log file after the file EEZEAR was deployed can be ignored.

Cleaning up from a failed installation

Installation can be canceled at any time. To recover from this situation, just run the installer again.

- Installation was canceled or failed before the installation was started: no cleanup is necessary
- Installation was canceled or failed during the installation phase: Run the uninstaller to clean up files that were installed on disk.
- Installation was canceled during the configuration phase: Installation can be resumed.
  If the system has to be cleaned up again, rerun the installer, and then run the uninstaller to undo all configuration steps and to remove all installed files from disk.
- Installation failed during the configuration phase: Corrective actions may be needed before installation can be resumed.
  You can also perform an uninstallation. If uninstall rather than resume is desired, the script uninstall.sh can be used to revert the configuration changes that have already been made. The installation log must be used to determine which changes were made and must be reverted. Afterwards, uninstall can be called to remove the files from the disk. Uninstall can be run with option -Dforce=true to be able to proceed even if errors are reported in the pre-uninstall phase.
  To just recover the files if the product was uninstalled but the unconfiguration was not successful and the files are needed to manually perform the remaining unconfiguration steps: Run the installer with the option -Dfilesonly=true in this case, only the files are installed; no configuration is performed
  Be sure to undo the configuration changes that were made during the installation before uninstalling. Otherwise, the configuration changes will be retained and the scripts to remove them are already uninstalled.
Procedures for troubleshooting an installation

If the installation fails, the installation wizard displays an error message.

When an error occurs, immediately archive the installation log files (see "Using the log file collector utility" on page 238). This ensures that the original log files are retained, which is important should you need to contact IBM Support, and you can use the archive for your own troubleshooting activities.

An error occurred in the pre-installation phase

If an error occurs in the pre-installation phase, that is, before the Install button was clicked, click the button Save installation log files to collect all installation log files. The zip file will be created at the location specified.

An error occurred in the installation phase

Typically, errors only occur in the installation phase if insufficient disk space is available.

An error occurred in the configuration phase:

Click Finish to finish the installation, then change to <EEZ_INSTALL_ROOT>/install and run the log file collector utility. The log zip will be created in the same directory. For details see "Using the log file collector utility" on page 238.

Using the log file collector utility

When an error occurs, use the you log file collector utility to collect the log files that were written during the installation. The utility generates an archive that you can use for your own troubleshooting activities and send to IBM Support if you cannot resolve the error.

Perform these steps to run the log file collector utility:

1. Change the directory to <EEZ_INSTALL_ROOT>/install.
2. Issue the following command:
   - Windows: collectinstallerlogs.bat
   - AIX/Linux: collectinstallerlogs.sh

   The command can be invoked with the option -D to only copy all logs (in case Java is not available); the directory tree created can then be packed manually

   Name of the file that is created by the utility:
   eezinstallerlogs_<timestamp>.zip

   On AIX and Linux, you can invoke the command with the option tar to use tar rather than jars for packing.

   The resulting archive has the following directory structure:
   - EEZ_logs
   - cfg: configuration files (for the automation engine, etc.)
   - logs: eezinstall.log, etc.
   - sh / bat (Linux/AIX: sh; Windows: bat): scripts used by installer
   - WAS_logs
   - logs: general WAS server logs
   - <server name>: logs for the selected WebSphere Application Server

Gathering information for IBM Support

If you cannot resolve an installation problem, send the installation log file archive to IBM support (see "Using the log file collector utility" on page 238).
Appendix E. Troubleshooting the installation of the HACMP adapter

Use this section for troubleshooting problems you experience when installing or configuring the HACMP adapter.

HACMP adapter does not start

Possible causes:
- HACMP level is lower than 5.3.0.5
  To check, use: ls1pp -l cluster.es.server.utils
- Cluster services have not been started
  Start the services using smitty: hacmp —> C-SPOC —> Manage...

HACMP adapter terminates

Cluster services terminated while the HACMP adapter was running
  If the adapter is automated, it should restart automatically on next priority node where cluster services run.

Adapter attempts to start but terminates again
  This may indicate that the adapter has not been configured correctly.

Adapter does not connect to the host

Make sure the firewall allows connections in both directions.

Check with netstat:
- whether the adapter listens on the request port (default port is 2001):
  netstat -an -f inet | grep 2001
  Output should be similar to:
  tcp 0 0 9.152.21.239:2001 :::* LISTEN
- whether the end-to-end automation manager or the Base component operations console listens on the event port (default port is 2002):
  AIX:
  netstat -an -f inet | grep 2002
  Linux:
  netstat -ant | grep 2002
  windows netstat -an and look exactly to the output as ther is no grep command
  Windows:
  netstat -an and look exactly to the output as ther is no grep command
  Output should be similar to:
  tcp 0 0 9.152.21.239:2002 :::* LISTEN

However, with netstat, you cannot check if tcp session creation is allowed or rejected by a firewall. To check if a tcp session can be created, use these approaches:
• Try to open a session with the telnet command to port 2001 from the end-to-end automation management host using this command:
  
  telnet <adapter-address> 2001

• Try to open a session with the telnet command to port 2002 from the first-level automation domain to the end-to-end automation management using this command:
  
  telnet <e2e-host> 2002

If the connections cannot be set up using telnet, a firewall may be blocking the sessions or other network problems, that is, routing problems, may exist.

HACMP adapter log files

Increasing the trace logging level

If your trace is not detailed enough to analyze a problem and the problem can be recreated, it may be useful to increase the trace logging level:

1. Invoke the adapter configuration dialog using cfghacadapter.
2. On the main panel of the configuration dialog, click Configure.
3. Select the Logger tab.
4. Set the Trace logging level to Maximum.
5. Click Apply. The new setting takes effect immediately.

For more information about the Logger tab, see “Logger tab” on page 189.

Log file locations

The HACMP adapter log files are located in the Tivoli Common Directory:

• Default location: /var.ibm/tivoli/common
• HACMP adapter-specific subdirectory structure in the Tivoli Common Directory:
  
  – eez/ffdc – Contains the First Failure Data Capture files (if the FFDC recording level is not set to Off in the adapter configuration dialog)
  – eez/logs – Contains the HACMP adapter trace file:
    - traceFlatAdapter.log
Appendix F. Troubleshooting the installation of the MSCS adapter

Use this section for troubleshooting problems you experience when installing or configuring the MSCS adapter.

**MSCS adapter log files**

This is where the adapter log files are located:

- **Tivoli Common Directory**
  - Default location: `C:\Program Files\IBM\tivoli\common`
  - MSCS adapter-specific subdirectory structure in Tivoli Common Directory:
    - `eez\ffdc` – Contains the First Failure Data Capture files (if the FFDC recording level is not set to Off in the adapter configuration dialog)
    - `eez\logs` – Contains the MSCS adapter log files:
      - `msgMSCSAdapter.log`
      - `traceMSCSAdapter.log` (if trace logging level is not set to Off)
      - `eventMSCSAdapter.log` (if trace logging level is not set to Off)
  - The default adapter installation directory is `C:\Program Files\IBM\tsamp\eez\mscs`.
  
Subdirectories and files used for troubleshooting:

- The file `data\eez.release.information.txt` is created in the adapter installation directory when the MSCS adapter is started. It contains information about service applied to the MSCS adapter and about the configuration settings used.
- The installation log files are located in the subdirectory `/install/logs`.

**MSCS adapter installation fails**

If the installation wizard indicates a problem, check the installer output and the following files for error messages:

- The log files in the subdirectory `/install/logs`.
- IBM Tivoli System Automation for Multiplatforms MSCS Adapter_install_log.log.
- `mscsinstall_<date_time>.log`

**Adapter configuration dialog problems occur**

A problem occurs using the adapter configuration dialog

Problem determination:

- The file `cfgmscsadapter.bat` contains a command for launching the configuration dialog
- The file contains a duplicate of this command which enables diagnostic output (option `-DEBUG`)

The Apply button on the Logger tab cannot be clicked

Possible cause: The MSCS adapter is not running.
Configuration files cannot be replicated
   Possible causes:
   • The MSCS cluster is not available.
   • The cluster contains only a single node.

Replication fails with the message "Login on target node failed"
   Possible cause: The domain user ID was not specified in the correct format,
   which is <user_ID>@<domain_name>.

MSCS adapter does not start

MSCS adapter does not start
   Problem determination:
   • The application event log should contain the message “The service SA
   MP MSCS Adapter has been started.”
   • In the configuration file cfg\mscs.service.properties, uncomment the
   property service-log-file, restart the service, and investigate the
   resulting file.
      Ensure to comment the property again before returning to normal
      operation.
   • Make sure that the correct user credentials are used for the SA MP
   MSCS Adapter Windows service. Re-enter the password for the service
   on the Log On tab of the service properties view, and restart the service.

The SA MP Adapter Service reports the status Started for some seconds and
   stops again
   • Startup should be completed within 60 seconds.
   • Refresh the view to see the actual status.
   Problem determination:
   • Investigate the MSCS adapter log file msgMSCSAdapter.log.
   • If no error messages can be found, increase the trace logging level to
   "Maximum" and provide all logs to IBM support.

The file msgMSCSAdapter.log contains the message EEZA0061E indicating that
   the adapter failed to bind to a socket
   Possible reason if the MSCS adapter service is made highly available using
   MSCS:
   • The network name or virtual IP address used for the “Automation
   adapter host” is not available during adapter startup
   Possible solution:
   • Check the spelling of the network name or virtual IP address in the
   adapter configuration dialog.
   • Check that there are appropriate “Network Name” / “IP Address”
   resources defined in MSCS and that they are working properly.
   • Check that the MSCS adapter service resource has a dependency on the
   “Network Name” / “IP Address” resources in MSCS.

MSCS adapter terminates

The MSCS adapter services stops and the log files contain no related error
   messages. In particular, message “EEZA0104I” does not appear in the MSCS
   adapter log file msgMSCSAdapter.log. The message indicates that the MSCS adapter
   was successfully stopped.
Problem determination:

1. Search for javacore.*.txt files in the subdirectory lib.
2. Use Windows tool drwtsn32 to configure dump capturing. Use the following settings:

![Image showing Dr. Watson for Windows configuration settings]

3. Try to recreate the MSCS adapter termination.
4. Provide the data to IBM support.

---

**Domain does not join**

The MSCS domain does not join within two minutes and the MSCS adapter service is no longer running

Problem determination:

- Investigate the MSCS adapter log file msgMSCSAdapter.log.
- If no problems can be found, increase the trace logging level to “Maximum” and provide all logs to IBM support.

The MSCS domain does not join within two minutes but the MSCS adapter service is running

Problem determination and possible causes:

- An invalid host name or IP address is specified for the end-to-end automation management server.
• The end-to-end automation management server cannot be reached from the system running the MSCS adapter. To check, use ping, telnet, and tracert commands.

• Determine the network name/IP address the MSCS adapter sends to the end-to-end automation management server:
  – Increase the trace logging level at least to “Minimum”, restart the MSCS adapter, investigate the log file eventMSCSAdapter.log.
  – Locate the latest adapter join event (“EVT_RSN=domainAdapterJoin”). The event contains the required information.

• The system running the MSCS adapter cannot be reached from the end-to-end server. To check, use ping, telnet, and tracert commands.

MSCS adapter uninstallation fails

Uninstaller indicates an uninstallation problem

This happens if the MSCS adapter service was still running during uninstallation.

Note: If the MSCS adapter service is made highly available using MSCS, MSCS may restart or fail over the service.

Uninstalling the MSCS adapter manually

Perform the steps in exactly this sequence:

1. Stop the MSCS adapter service and ensure that it is not restarted by MSCS on the system where the manual uninstallation is performed.

2. Manually remove the service by issuing the command:
   sc.exe delete "SA MP MSCS Adapter"

3. Manually remove the service JaasLogon by issuing the following commands:
   cd <adapter_installation_directory>\jre\bin
   JaasLogon.exe -remove

4. Delete the adapter installation directory.

5. If no other Tivoli System Automation product is installed on the system, you can delete the eez subdirectories of the Tivoli Common Directory.

6. If no other products that were installed with InstallAnywhere still exist on the system, go to C:\Program Files\Zero G Registry and delete the complete directory. If other InstallAnywhere installer products are installed, you must remove all entries related to MSCS Adapter from the file .com.zerog.registry.xml.

   For the following example, all subelements of <products> and <components> must be deleted

Example:

<?xml version="1.0" encoding="UTF-8"?>
<registry install_date="2007-06-19 13:13:59" version="1.1"
 last_modified="2007-06-21 16:26:20">
 <products>
  <product name="IBM Tivoli System Automation for Multiplatforms MSCS Adapter"
 id="65d4e8-1e4-11b2-9a39-0e2f5b28587" version="2.3.0.0" copyright="2007" info_url="" support_url=""
 location="C:\Program Files\IBM\tamp\eez\mscs"
 last_modified="2007-06-21 12:35:58">
   <vendor name="IBM" id="4b891a0-1ee0-11b2-8c02-f523645d652c"
 home_page="" email=""/>
 </product>
 </products>
Appendix G. Using IBM Support Assistant

IBM Support Assistant is a free, stand-alone application that you can install on any workstation. IBM Support Assistant saves you time searching product, support, and educational resources and helps you gather support information when you need to open a problem management record (PMR) or Electronic Tracking Record (ETR), which you can then use to track the problem.

You can then enhance the application by installing product-specific plug-in modules for the IBM products you use. The product-specific plug-in for IBM Tivoli System Automation for Multiplatforms provides you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

Installing IBM Support Assistant and the Tivoli System Automation for Multiplatforms plug-in

To install the IBM Support Assistant V3.0, complete these steps:

- Go to the IBM Support Assistant Web Site:
- Download the installation package for your platform. Note that you will need to sign in with an IBM user ID and password (for example, a MySupport or developerWorks® user ID). If you do not already have an IBM user ID, you may complete the free registration process to obtain one.
- Uncompress the installation package to a temporary directory.
- Follow the instructions in the Installation and Troubleshooting Guide, included in the installation package, to install the IBM Support Assistant.

To install the plug-in for IBM Tivoli System Automation for Multiplatforms, complete these steps:

1. Start the IBM Support Assistant application. IBM Support Assistant is a Web application that is displayed in the default, system configured Web-browser.
2. Click the Updater tab within IBM Support Assistant.
3. Click the New Products and Tools tab. The plug-in modules are listed by product family.
5. Select the features you want to install and click Install. Be sure to read the license information and the usage instructions.
6. Restart IBM Support Assistant.
Appendix H. 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.

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
Mail Station P300
2455 South Road
Poughkeepsie New York 12601-5400
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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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 may 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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

**Trademarks**

- IBM, the IBM logo, ibm.com, AIX, DB2, developerWorks, HACMP, NetView, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, WebSphere, and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. IBM Redbooks and the IBM Redbooks logo are registered trademarks of IBM.
- Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated 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.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat and all Red Hat-based trademarks are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Other company, product, and service names may be trademarks or service marks of others.
Index

**A**

automation adapter 159
automation manager 159
maximum number of connections 115

**B**

Base component 9
installation prerequisites 6
Korn shell 6
installing 3
installing services 67
operations console 26
supported platforms 19
uninstalling 42
preparing for installation 6
supported languages 11
uninstalling 41
Base component for AIX and Linux 9
installing 9
planning for the installation 3
supported platforms 4
upgrading 9
Base component on AIX and Linux coexistence with other products 3

**C**

can sets 11
supported by Base component 11
supported by the End-to-End Automation Management component 95
Cluster Systems Management (CSM) 11
coexistence with the Base component 3
configuration dialog 119
end-to-end automation manager 119
configuration properties 119
end-to-end automation manager 119

**D**

DB2 86
automation manager database creating 86
installation parameters 91
server installation 84
setup options 79
local setup 79
remote setup 79
software prerequisites for remote setup 81
local setup 81
WebSphere Application Server requests 112
disk space requirements 83
AIX 83
Linux 83
Windows 82

**E**

e2einstallerlogs 238, 245
log file collector utility 244
NoClassDefFoundError 244
electronic distribution 76
end-to-end automation adapter 159
adapter tab 163
automating the adapter 161, 167
automation policy 177
configuration 163
configuration for the operations console 39
defining the policy 176
logger tab 172
overview 160
replicating configuration files 175
security tab 170
end-to-end automation domain name 94
end-to-end automation engine WebSphere Application Server user ID 94
End-to-End Automation Management component 95
supported languages 95
supported operating systems 79
troubleshooting 243
uninstalling 143
end-to-end automation manager configuration dialog 119
configuring 119

**F**

first-level automation domain 157
fix packs 67
installing 139

**G**

General Parallel File System (GPFS) 11
coexistence with the Base component 3

**H**

HACMP adapter 180, 186
automating 180
configuration 193
policy 193
removing 193

HACMP adapter (continued)
configuration 194
configuration dialog 182
Adapter tab 182
Automation tab 186
Host using adapter tab 184
invoking 181
Logger tab 189
Security tab 188
using 182
configuration directory 179
configuring 181
installation directory 179
installation source directory 179
installing 179
prerequisites 179
using SMIT 179
log file locations 248
packaging 179
replicating configuration files 192
saving the configuration 191
trace logging level 248
troubleshooting 247
home page 179
IBM Tivoli System Automation 139
host using the adapter 161
HTTP session timeout 114
modifying 114

**I**

IBM Tivoli Enterprise Console 94
installation parameters 94
IBM Tivoli System Automation 94
Base component for AIX and Linux supported platforms 4
migrating 12
installation planning 75
post-installation tasks 114
prerequisites 96
product CD 75
verifying 111
installation directory 21, 90
installing 9
Base component for AIX and Linux service fix packs 67, 139
installing IBM Tivoli System Automation 94
initial configurations 7
uninstalling service 71
installing service 9
Base component 67
Base component operations console 67
installing the Base component 3

© Copyright IBM Corp. 2006, 2007
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>license</td>
</tr>
<tr>
<td></td>
<td>installing 11</td>
</tr>
<tr>
<td></td>
<td>Try &amp; Buy, upgrading 11</td>
</tr>
<tr>
<td></td>
<td>log file collector utility 238, 245</td>
</tr>
<tr>
<td></td>
<td>LTPA settings</td>
</tr>
<tr>
<td></td>
<td>LTPA password 114</td>
</tr>
<tr>
<td></td>
<td>LTPA timeout 114</td>
</tr>
<tr>
<td>M</td>
<td>middleware software CDs</td>
</tr>
<tr>
<td></td>
<td>contents 84</td>
</tr>
<tr>
<td></td>
<td>migrating IBM Tivoli System Automation</td>
</tr>
<tr>
<td></td>
<td>Base component 12</td>
</tr>
<tr>
<td></td>
<td>completing the migration 15</td>
</tr>
<tr>
<td></td>
<td>migrating a node step by step 13</td>
</tr>
<tr>
<td></td>
<td>migrating an entire domain 13</td>
</tr>
<tr>
<td></td>
<td>MSCS adapter</td>
</tr>
<tr>
<td></td>
<td>configuring 201</td>
</tr>
<tr>
<td></td>
<td>high availability</td>
</tr>
<tr>
<td></td>
<td>planning 199</td>
</tr>
<tr>
<td></td>
<td>providing 210</td>
</tr>
<tr>
<td></td>
<td>installation directory 249</td>
</tr>
<tr>
<td></td>
<td>installation log files 249</td>
</tr>
<tr>
<td></td>
<td>installation wizard 199</td>
</tr>
<tr>
<td></td>
<td>installing 199</td>
</tr>
<tr>
<td></td>
<td>log files 249</td>
</tr>
<tr>
<td></td>
<td>logging 206</td>
</tr>
<tr>
<td></td>
<td>packaging 198</td>
</tr>
<tr>
<td></td>
<td>prerequisites 198</td>
</tr>
<tr>
<td></td>
<td>replicating configuration files 209</td>
</tr>
<tr>
<td></td>
<td>security 205</td>
</tr>
<tr>
<td></td>
<td>silent mode installation 201</td>
</tr>
<tr>
<td></td>
<td>tracing 206</td>
</tr>
<tr>
<td></td>
<td>troubleshooting 249</td>
</tr>
<tr>
<td></td>
<td>uninstalling 216</td>
</tr>
<tr>
<td></td>
<td>verifying the installation 216</td>
</tr>
<tr>
<td>N</td>
<td>NoClassDefFoundError</td>
</tr>
<tr>
<td></td>
<td>eezinstall.log 244</td>
</tr>
<tr>
<td>O</td>
<td>operations console</td>
</tr>
<tr>
<td></td>
<td>CDs and archives 3</td>
</tr>
<tr>
<td></td>
<td>configuration for direct access mode 39</td>
</tr>
<tr>
<td></td>
<td>configuration script 39</td>
</tr>
<tr>
<td></td>
<td>Configuring the end-to-end automation adapter 39</td>
</tr>
<tr>
<td></td>
<td>disk space requirements 20</td>
</tr>
<tr>
<td></td>
<td>installation parameters 23</td>
</tr>
<tr>
<td></td>
<td>installation steps 26</td>
</tr>
<tr>
<td></td>
<td>installing service 67</td>
</tr>
<tr>
<td></td>
<td>packaging CDs and archives 17</td>
</tr>
<tr>
<td></td>
<td>planning the configuration 39</td>
</tr>
<tr>
<td></td>
<td>product prerequisites 19</td>
</tr>
<tr>
<td></td>
<td>troubleshooting 237</td>
</tr>
<tr>
<td>P</td>
<td>packaging</td>
</tr>
<tr>
<td></td>
<td>product CD 75</td>
</tr>
<tr>
<td></td>
<td>post-installation tasks</td>
</tr>
<tr>
<td></td>
<td>modifying the LTPA settings 114</td>
</tr>
<tr>
<td></td>
<td>overview 114</td>
</tr>
<tr>
<td></td>
<td>product CD contents 95</td>
</tr>
<tr>
<td></td>
<td>directories 95</td>
</tr>
<tr>
<td></td>
<td>installation wizard files 75</td>
</tr>
<tr>
<td>R</td>
<td>release notes 67, 139</td>
</tr>
<tr>
<td></td>
<td>RSCTMM 58</td>
</tr>
<tr>
<td></td>
<td>RSCTNLV 58</td>
</tr>
<tr>
<td>S</td>
<td>SA operations console</td>
</tr>
<tr>
<td></td>
<td>initial user ID 94</td>
</tr>
<tr>
<td></td>
<td>SAMMM 58</td>
</tr>
<tr>
<td></td>
<td>SAMNLV 58</td>
</tr>
<tr>
<td></td>
<td>security concepts overview 83</td>
</tr>
<tr>
<td></td>
<td>SSL 83</td>
</tr>
<tr>
<td></td>
<td>service installing 67, 139</td>
</tr>
<tr>
<td></td>
<td>SSL security concepts 83</td>
</tr>
<tr>
<td></td>
<td>support site IBM Tivoli System Automation 139</td>
</tr>
<tr>
<td></td>
<td>supported platforms Base component for AIX and Linux 4</td>
</tr>
<tr>
<td>T</td>
<td>TCP/IP connectivity</td>
</tr>
<tr>
<td></td>
<td>hardware requirements 82</td>
</tr>
<tr>
<td></td>
<td>Telnet dialog buffer 7</td>
</tr>
<tr>
<td></td>
<td>testing</td>
</tr>
<tr>
<td></td>
<td>connection between WebSphere Application Server and DB2 112</td>
</tr>
<tr>
<td></td>
<td>timeouts HTTP session timeout 114</td>
</tr>
<tr>
<td></td>
<td>LTPA timeout 114</td>
</tr>
<tr>
<td></td>
<td>Tivoli Common Directory 21, 90</td>
</tr>
<tr>
<td></td>
<td>Tivoli Event Integration Facility (EIF) 157</td>
</tr>
<tr>
<td></td>
<td>trademarks 258</td>
</tr>
<tr>
<td></td>
<td>troubleshooting End-to-End Automation Management component 243</td>
</tr>
<tr>
<td></td>
<td>HACMP adapter 247</td>
</tr>
<tr>
<td></td>
<td>MSCS adapter 249</td>
</tr>
<tr>
<td></td>
<td>operations console, Base component 237</td>
</tr>
<tr>
<td>U</td>
<td>uninstalling Base component</td>
</tr>
<tr>
<td></td>
<td>operations console 42</td>
</tr>
<tr>
<td></td>
<td>End-to-End Automation Management component 143</td>
</tr>
<tr>
<td>V</td>
<td>VCS adapter</td>
</tr>
<tr>
<td></td>
<td>automating 218, 224</td>
</tr>
<tr>
<td></td>
<td>automation policy defining 231</td>
</tr>
<tr>
<td></td>
<td>removing 231</td>
</tr>
<tr>
<td></td>
<td>configuration verifying 231</td>
</tr>
<tr>
<td></td>
<td>configuration dialog Adapter tab 221</td>
</tr>
<tr>
<td></td>
<td>Automation tab 224</td>
</tr>
<tr>
<td></td>
<td>Host using adapter tab 222</td>
</tr>
<tr>
<td></td>
<td>invoking 220</td>
</tr>
<tr>
<td></td>
<td>Logger tab 227</td>
</tr>
<tr>
<td></td>
<td>Security tab 226</td>
</tr>
<tr>
<td></td>
<td>using 221</td>
</tr>
<tr>
<td></td>
<td>configuring 220</td>
</tr>
<tr>
<td></td>
<td>installation source directory 217</td>
</tr>
<tr>
<td></td>
<td>installation steps 217</td>
</tr>
<tr>
<td></td>
<td>installing 217</td>
</tr>
<tr>
<td></td>
<td>prerequisites 217</td>
</tr>
<tr>
<td></td>
<td>packaging 217</td>
</tr>
<tr>
<td></td>
<td>replicating configuration files 230</td>
</tr>
<tr>
<td></td>
<td>saving the configuration 229</td>
</tr>
<tr>
<td></td>
<td>verifying the version number 14</td>
</tr>
<tr>
<td></td>
<td>version number of IBM Tivoli System Automation 14</td>
</tr>
<tr>
<td>W</td>
<td>Web browsers requirements 20, 81</td>
</tr>
<tr>
<td></td>
<td>WebSphere Application Server connection to DB2 test 112</td>
</tr>
<tr>
<td></td>
<td>installation parameters 93</td>
</tr>
<tr>
<td></td>
<td>installing 87</td>
</tr>
<tr>
<td></td>
<td>Fix Pack 9 89</td>
</tr>
<tr>
<td></td>
<td>Version 6.1.0.0 88</td>
</tr>
<tr>
<td></td>
<td>interim fixes 139</td>
</tr>
<tr>
<td></td>
<td>server1 78</td>
</tr>
<tr>
<td></td>
<td>Upgrade CD 76</td>
</tr>
</tbody>
</table>
Readers’ Comments — We’d Like to Hear from You

System Automation for Multiplatforms
Installation and Configuration Guide
Version 2.3

Publication No. SC33-8273-02

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.
Submit your comments using one of these channels:
• Send your comments to the address on the reverse side of this form.
• Send a fax to the following number: FAX (Germany): 07031+16-3456
  FAX (Other Countries): (+49)+7031-16-3456
• Send your comments via e-mail to: eservdoc@de.ibm.com

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

E-mail address