CA Workload Automation AE

UNIX Implementation Guide

r11.3

CA Technologies Product References

This document references the following CA Technologies products:

- CA Access Control
- CA AutoSys Workload Automation Connect Option (CA AutoSys WA Connect Option)
- CA Embedded Entitlements Manager (CA EEM)
- CA Job Management Option
- CA Jobtrac™ Job Management (CA Jobtrac JM)
- CA Network and Systems Management (CA NSM)
- CA NSM Event Management
- CA NSM Management Command Center (CA NSM MCC)
- CA Scheduler® Job Management (CA Scheduler JM)
- CA Service Desk
- CA Spectrum Automation Manager (formerly named CA DCA Manager)
- CA Universal Job Management Agent (CA UJMA)
- CA Workload Automation AE (formerly named CA AutoSys Workload Automation)
- CA Workload Automation Agent for UNIX (CA WA Agent for UNIX)
- CA Workload Automation Agent for Linux (CA WA Agent for Linux)
- CA Workload Automation Agent for Windows (CA WA Agent for Windows)
- CA Workload Automation Agent for i5/OS (CA WA Agent for i5/OS)
- CA Workload Automation Agent for Application Services (CA WA Agent for Application Services)
- CA Workload Automation Agent for Web Services (CA WA Agent for Web Services)
- CA Workload Automation Agent for Databases (CA WA Agent for Databases)
- CA Workload Automation Agent for SAP (CA WA Agent for SAP)
- CA Workload Automation Agent for PeopleSoft (CA WA Agent for PeopleSoft)
- CA Workload Automation Agent for Oracle E-Business Suite (CA WA Agent for Oracle E-Business Suite)
- CA Workload Automation Agent for z/OS (CA WA Agent for z/OS)
- CA Workload Automation EE (formerly named CA ESP Workload Automation)
- CA Workload Automation SE (formerly named CA 7 Workload Automation)

- CA Workload Control Center (CA WCC)
- CA Desktop and Server Management (CA DSM)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 3: Installation Preparation 47

Chapter 4: Installation Considerations 57

Chapter 5: Installing the Server 67

Chapter 13: Configuring CA Workload Automation AE to Work with the Agent 163

Chapter 14: Configuring CA Workload Automation AE to Work with CA Common Components 195

Chapter 1: Introduction

Welcome to CA Workload Automation AE, the scheduling and operations automation software for distributed computing environments.

This document provides an overview of CA Workload Automation AE and describes how to install and configure components, dual event servers, and high availability options, and set up database connections. It also contains information about advanced configurations and upgrading an existing installation.

This section contains the following topics:

Intended Audience

This document is for system administrators who are responsible for upgrading, installing, and configuring CA Workload Automation AE on UNIX. It assumes familiarity with the operating system and with the database server you use.

Note: The UNIX instructions in this document also apply to Linux systems unless otherwise noted.

CA Workload Automation AE

CA Workload Automation AE is an automated job control system for scheduling, monitoring, and reporting.

A *job* is any single command, executable, script, or batch file. These jobs can reside on any configured machine that is attached to a network. Corresponding job definitions contain a variety of qualifying attributes for associated jobs, including the conditions specifying when and where a job should run.

There are many ways to define and implement jobs. It is likely that the way you use CA Workload Automation AE to address your distributed computing needs will evolve over time. As you become more familiar with the CA Workload Automation AE features and the characteristics of your jobs, you can refine your use of CA Workload Automation AE.

Before you install and use CA Workload Automation AE, however, it is important to understand the basic system, its components, and how these components work together.

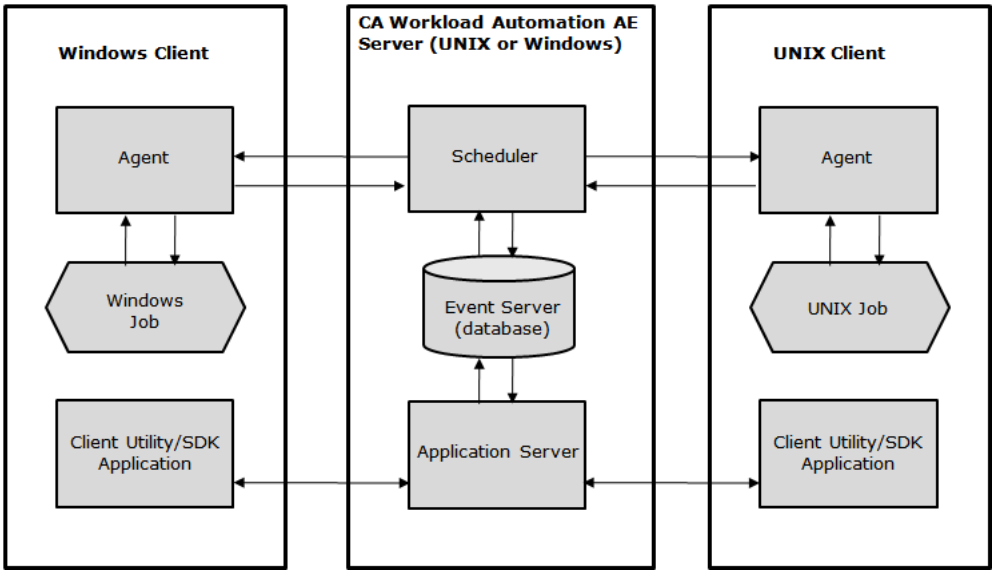
CA Workload Automation AE Components

The main CA Workload Automation AE components are as follows:

- Event server
- Application server
- Scheduler
- Client
- Agent

CA Workload Automation AE also provides utilities to help you define, run, and maintain instances and jobs. The client utilities enable you to define, manage, monitor, and report on jobs.

The following illustration shows the components in a basic configuration and displays the communication paths between them:



Event Server

The e*vent server*, or database, is the data repository for all events and system information. It also serves as a repository for all job, monitor, and report definitions.

Occasionally, the database is called a data server, which actually describes a server instance. That is, it is a UNIX process or a Windows service and associated data space (or raw disk storage), which can include multiple databases or tablespaces.

You can configure CA Workload Automation AE to run using two databases, or *dual event servers*. This feature provides complete redundancy. Therefore, if you lose one event server, operations can continue on the second event server without loss of information or functionality.

Application Server

The *application server* acts as the communication interface between the event server and the client utilities. It receives requests from the client utilities, queries the event server, and returns the responses to the client utilities.

Scheduler

The *scheduler* is the program, running as a UNIX daemon process or a Windows service, that runs CA Workload Automation AE. It processes all the events it reads from the event server.

When you start the scheduler, it continually scans the database for events to process. For example, when the scheduler finds a STARTJOB event, it verifies whether the event satisfies the starting conditions for that job in the database. Based on this information, the scheduler determines the actions to take and instructs the appropriate agent to perform the actions. These actions may include starting or stopping jobs, checking for resources, monitoring existing jobs, or initiating corrective procedures.

You can set up a second scheduler, called the s*hadow scheduler*. If the primary scheduler fails for some reason, the shadow scheduler takes over the responsibility of interpreting and processing events.

If you run CA Workload Automation AE with a shadow scheduler and dual event servers, a *tie-breaker scheduler* is required. It is a scheduler process that runs on a third node. The tie-breaker scheduler remains permanently idle and updates the event servers periodically to indicate its presence. It resolves contentions and eliminates situations in which one scheduler takes over because its own network is down.

More information:

Shadow and Tie-breaker Schedulers (see page 26)

Client

A *client* is any executable that interfaces with the application server. This includes CA Workload Automation AE Command Line Interface (CLI) applications such as Job Information Language (JIL) and autorep. It also includes the CA WCC services, which are clients of the application server and service the CA WCC GUI components, and any user-defined binaries that link to the CA Workload Automation AE SDK.

Client applications work by calling Application Programming Interfaces (APIs) that are available in the application server. A client can run anywhere in the enterprise provided it can reach the computer where the application server is running. It does not require the installation of a database vendor client. Clients are the means by which users control the scheduling environment by creating and monitoring the scheduling resources.

Note: For more information about the CA Workload Automation AE SDK APIs, see the *API Reference Guide*.

Agents and Agent Plug-ins

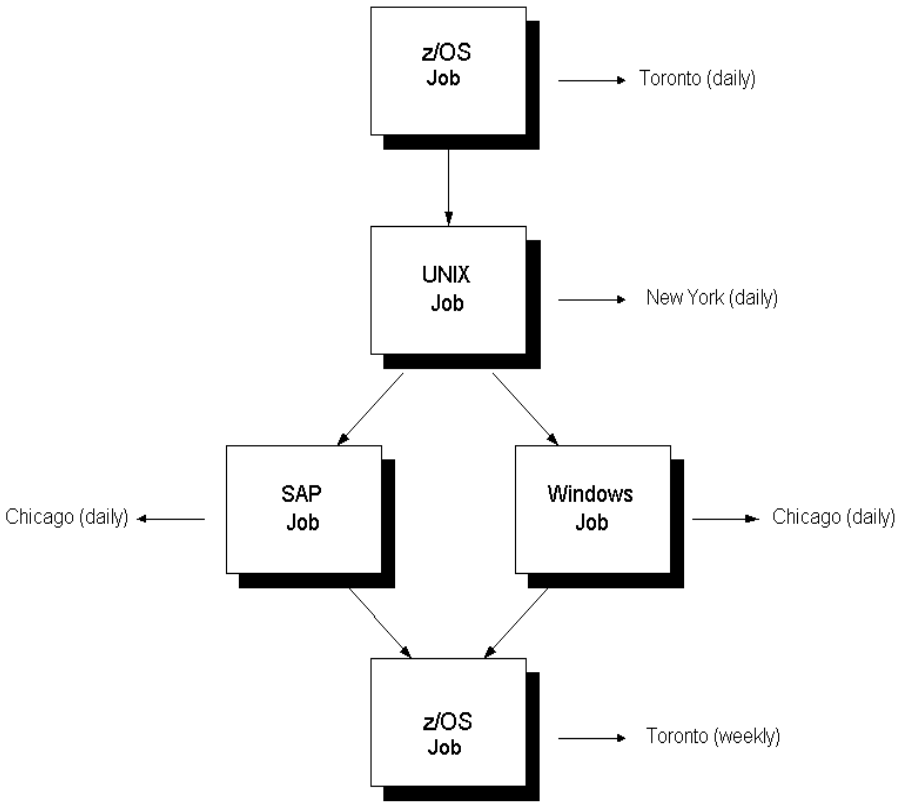
Agents are the key integration components of CA workload automation products. Agents let you automate, monitor, and manage workload on all major platforms, applications, and databases. To run workload on a particular system, you install an agent on that system. If your workload must run on a UNIX computer, for example, you can install and configure the CA WA Agent for UNIX. The agent lets you run UNIX scripts, execute UNIX commands, transfer files using FTP, monitor file activity on the agent computer, and perform many other tasks.

You can extend the functionality of the agent by installing one or more agent plug-ins in the agent installation directory. If you have a relational database such as Oracle, for example, you can install a database agent plug-in to query and monitor the database. Other agent plug-ins are also available. For more information, see the *Implementation Guide* for the appropriate agent plug-in.

Note: The agent plug-ins are only available for UNIX, Linux, and Windows operating environments.

Example: Workload with Different Types of Jobs

The following workload contains z/OS jobs, a UNIX job, an SAP job, and a Windows job, running on different computers, in different locations, and at different times:



Interface Components

You can use the client utilities or CA WCC to define, monitor, and report on jobs.

Note: For more information, see the CA WCC documentation.

How the Event Server, Scheduler, and Agent Interact

The following steps explain the interactions between the event server, scheduler, and agent:

1. From the event server, the scheduler reads a new event, which is a STARTJOB event with a start time condition that has been met. Then, the scheduler reads the appropriate job definition from the database and, based on that definition, determines what action to take. In the example, the scheduler runs the following command on WorkStation_2:
   - On UNIX:

     ```
     rm /tmp/mystuff/*
     ```

   - On Windows:

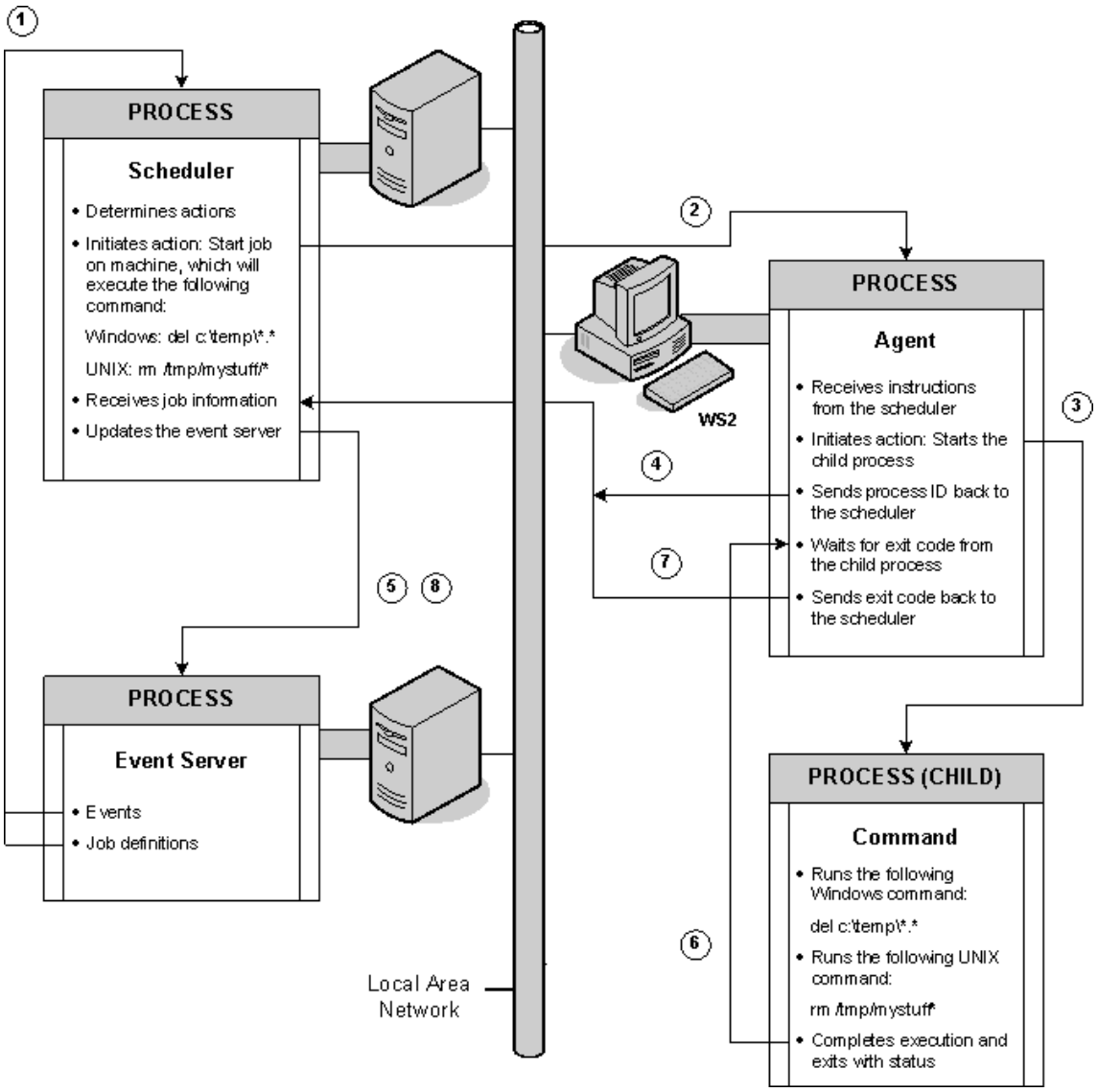
     ```
     del C:\tmp\*.*
     ```

2. The scheduler communicates with the agent on WorkStation_2. The agent receives the instructions to run the job.
3. The agent performs resource checks and creates a process that actually runs the specified command.
4. The agent communicates the job execution information (such as the process ID, agent log file name, job output log file name, and so on) to the scheduler.
5. The scheduler converts the job execution information into a job event and updates the event server with the event information.
6. The command completes and exits, and the agent captures the command's exit code.
7. The agent communicates the job completion information (such as exit code, status, and so on) to the scheduler.
8. The scheduler converts the job completion information into a job event and updates the event server with the event information.

The scheduler and the event server must be running to make CA Workload Automation AE fully operational.

Example: Interaction Between the Event Server, Scheduler, and Agent

This example illustrates the event server, scheduler, and agent running on different computers. At a start date and time specified in the job definition, suppose you run the command shown in the illustration on WorkStation_2 (WS2):



Notes:

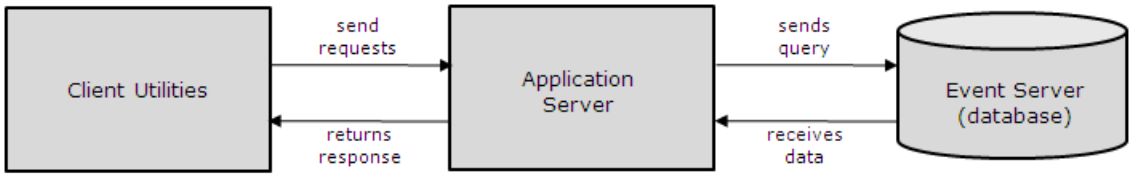
- The application server communicates with the agent only when client utilities like chase and autoping are run or when jobs contain globs or blobs as input or output.
- The scheduler and the event server typically run on the same computer.

How the Event Server, Application Server, and Client Utilities Interact

The following steps explain the interactions between the event server, application server, and client utilities:

1. The client utilities send requests to the application server.
2. The application server executes the request (for example, inserting a job) which results in information either being inserted, updated, retrieved, or removed from the event server. The responses are returned to the client as the operation executes or after the operation completes.

The following illustration shows how the event server, application server, and client utilities interact.



Note: The application server communicates with the agent only when client utilities like chase and autoping are run or when jobs contain globs or blobs as input or output.

Example: Interaction Between the Event Server, Application Server, and Client Utilities

Suppose that you issue the autorep command at an UNIX operating system prompt or the Windows instance command prompt, the event server, application server, and the client utilities interact with each other as follows:

1. The autorep client sends a request to the application server.
2. The application server queries the database, receives the data from the event server, prepares one or more responses, and sends all the responses to the autorep client.
3. The autorep client receives all the responses and displays the report.

Instance

A CA Workload Automation AE *instance* is a licensed version of CA Workload Automation AE software running as a server with one or more clients or agents. Clients and agents can run on a single computer or on multiple computers. An instance uses its own scheduler, application server, and event server and operates independently of other instances.

The instance ID (an uppercase, three-character alphanumeric name) that is referenced by the AUTOSERV environment variable identifies a CA Workload Automation AE server installation on a particular computer. The default instance ID is ACE. However, you can specify a different ID only during installation.

Multiple instances can run on the same computer, but they must have different instance IDs. For example, you can have one instance for production and another for development. Multiple instances can run on the same computer using a single copy of the binaries, and can schedule jobs on the same computers without interfering or affecting other instances.

Note: Additional instances can be added at a later time by running the wa_setup.sh script.

Computers Used

From a hardware perspective, the CA Workload Automation AE architecture comprises the following types of computers attached to a network:

- Server computer—The s*erver* is the computer on which the scheduler and the application server reside.
- Client computer—The c*lient* is the computer on which the client software resides.
- Agent computer—The a*gent* is the computer on which the agent software resides. An agent is installed on the computer with the scheduler, and it can also be installed on separate physical computers.

The Configuration File

Each instance has the following configuration file:

```
$AUTOUSER/config.$AUTOSERV
```

The $AUTOSERV value is the name of the instance with which the configuration file is associated. Upon startup, CA Workload Automation AE reads the configuration file to determine its behavior, including which databases to connect to and how to react to certain error conditions. Also, the run-time behavior of the scheduler is based on the parameters in this configuration file.

Note: For more information about the parameters in the configuration file, see the *Administration Guide*.

CA Workload Automation AE High Availability Options

CA Workload Automation AE provides the following high availability options that let the product keep processing even if an event server or scheduler, or both, fail due to hardware or connection problems:

- Dual event servers
- Shadow and tie-breaker scheduler

You can install and configure the high availability options during the CA Workload Automation AE installation, or you can modify an existing installation to add the high availability options.

The high availability options are controlled by parameters in the $AUTOUSER/config.$AUTOSERV configuration file.

More information:

Shadow and Tie-Breaker Schedulers (see page 275)
Dual Event Servers (see page 267)

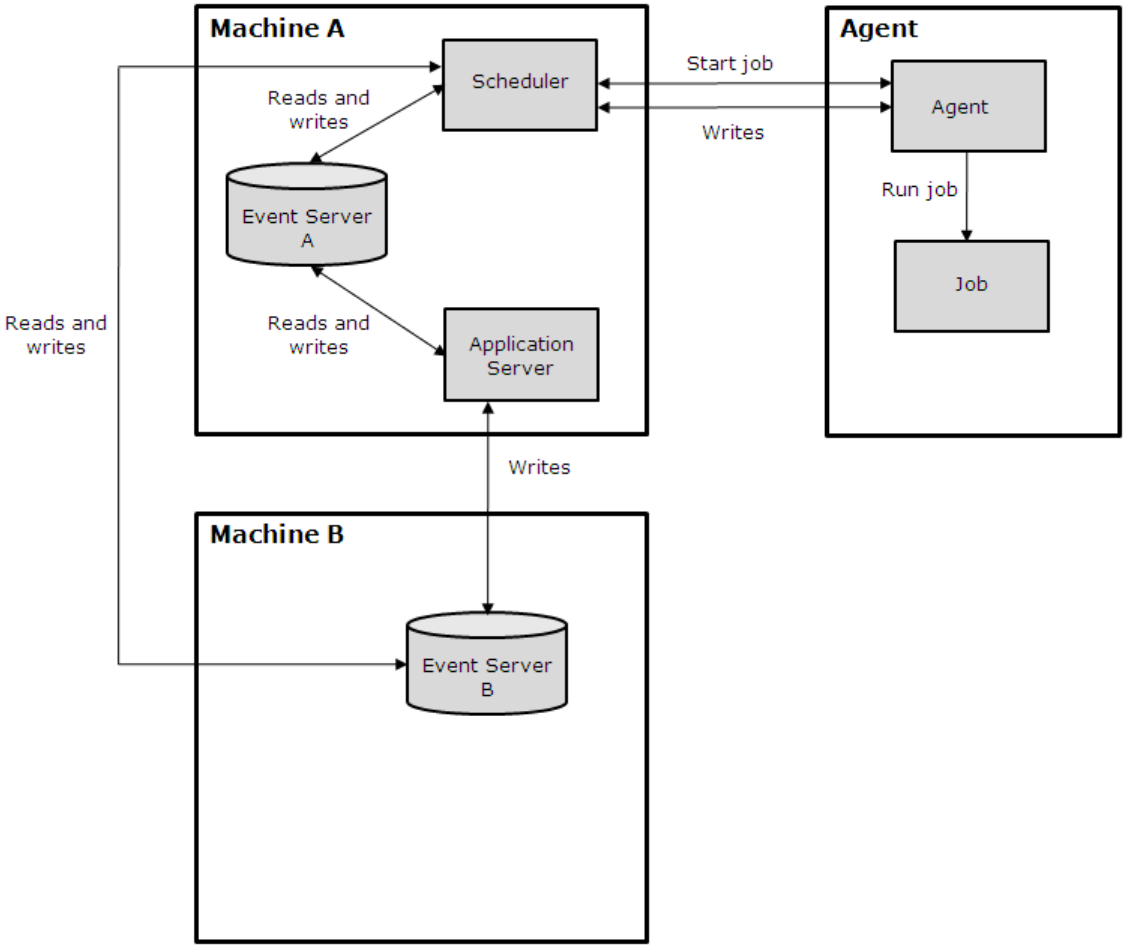
Dual Event Servers

One way that CA Workload Automation AE provides high availability is by running two event servers that contain identical information, including job definitions and events. With the dual event server option, CA Workload Automation AE reads and writes to both servers simultaneously. The product also keeps both event servers synchronized and provides complete recovery when one server becomes unusable, disabled, or corrupted.

When processing events, the scheduler reads from both event servers. If it detects an event only on one server, it copies the missing event to the other server. This feature lets event processing continue uninterrupted.

In addition, the agent sends events to the scheduler. The scheduler then writes to both event servers.

The following illustration shows a typical configuration running with dual event servers:



Running Dual Event Server Mode

When the scheduler detects an unrecoverable condition on one of the event servers while running in dual event server mode, it automatically rolls over to single event server mode. A rollover results from one of the following conditions:

- The connection to the database is lost and, after the configured number of reconnection attempts, the database remains unconnected.
- The database has an unrecoverable error. For example, the database is corrupt or a media failure occurs.

If there was an event server rollover on servers running on UNIX, the scheduler edits the $AUTOUSER/config.$AUTOSERV configuration file, on the server computer only, to comment out the database that has been taken offline. The scheduler makes this change so that the utilities attempting to access the database know that CA Workload Automation AE is now running in single event server mode.

Note: If CA Workload Automation AE is configured to run with dual event servers, the scheduler will not start unless both the databases are available.

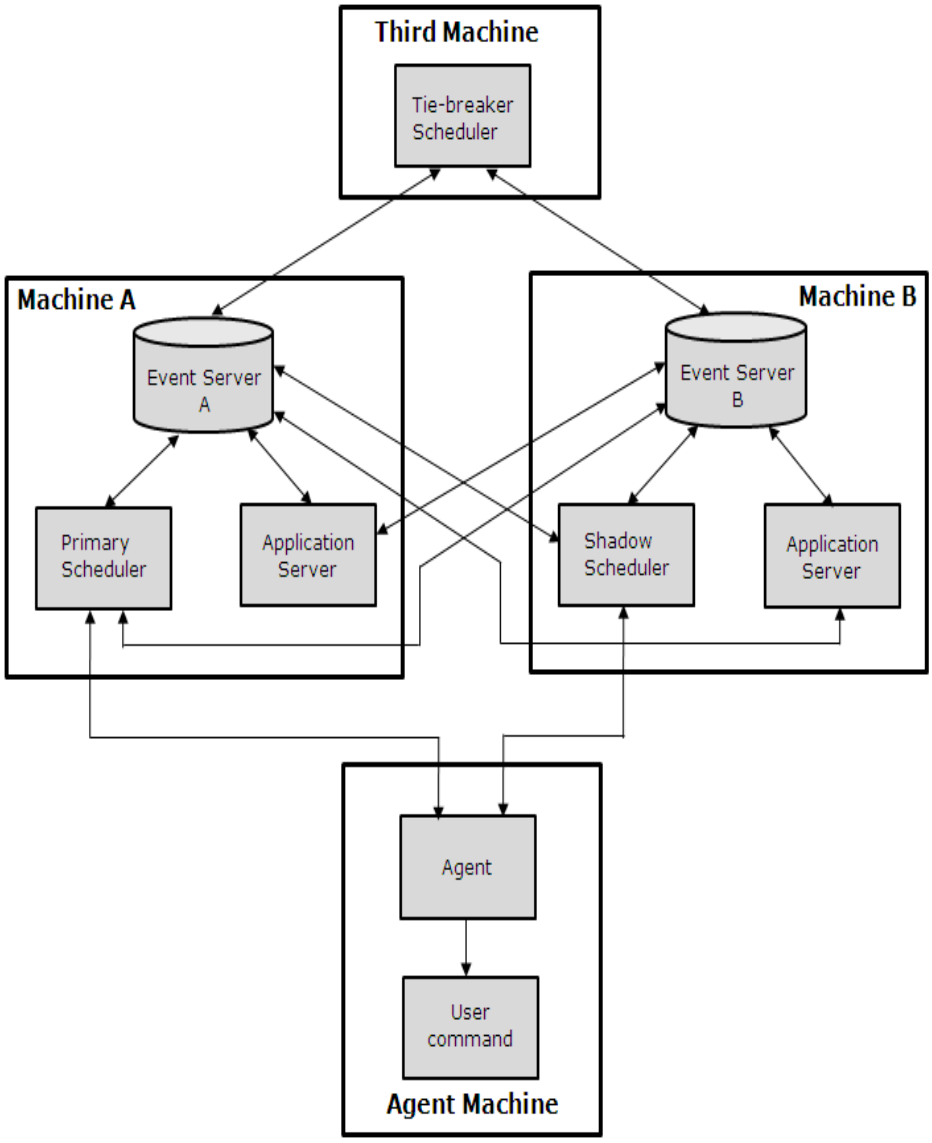
Before restarting the server that is down, you must make sure that the two event servers are synchronized.

Note: For information about event server recovery and how to synchronize event servers, see the *Administration Guide*.

Shadow and Tie-breaker Schedulers

Another way that CA Workload Automation AE provides high availability is by running with a shadow scheduler. The shadow scheduler is designed to take over scheduling if the primary scheduler fails. The tie-breaker scheduler then resolves contentions and eliminates situations in which one scheduler takes over because its own network is down. The shadow scheduler and dual event servers are independent features, but you can run them together.

The following illustration shows a typical configuration running with the primary and shadow schedulers and dual event servers:



Notes:

- The application server communicates with the agent only when client utilities like chase is run or when jobs contain globs or blobs as input or output.
- We recommend that the primary, shadow, and tie-breaker schedulers reside on different computers to prevent a single point of failure.

Running with a Shadow Scheduler

The shadow scheduler typically stays in idle mode, checking the database for routine database updates from the primary and tie-breaker schedulers, which indicate that workload scheduling is processing normally. If the shadow scheduler stops seeing updates to the database, it assumes that the primary scheduler has failed.

When the shadow scheduler does not see an update from the primary scheduler, it checks for the tie-breaker scheduler update to the database. If it cannot find an update, the shadow scheduler shuts down. If it can, the shadow scheduler attempts to signal the primary scheduler to stop and takes over event processing.

Similarly, if the primary scheduler cannot locate an update from the shadow scheduler, it checks for the tie-breaker scheduler update to the database. If it cannot find an update, the primary scheduler shuts down. If it can, the primary scheduler attempts to signal the shadow scheduler to stop and takes over event processing.

If it is necessary at the time of scheduler rollover, CA Workload Automation AE also switches over from dual event server mode to single event server mode. That is, if the primary scheduler and an event server are on the same computer, the scheduler failure could also mean an event server failure. In this situation, CA Workload Automation AE switches over to the shadow scheduler and to single event server mode.

In some cases, such as when there are network problems, CA Workload Automation AE may not be able to determine which scheduler is the functional one. In this case, both the schedulers shut down.

Note: For more information about scheduler rollover and recovery, see the *Administration Guide*.

CA Workload Automation AE in a Cluster

There are several brands of clustering software for UNIX systems that provide mechanisms for making applications highly-available. The same principles apply to configuring CA Workload Automation AE in any of them.

Each cluster system has a way to associate a movable host name with one or more server applications. Some cluster systems use an alias IP address assigned to the computer currently running the application. Others use a dynamic name service to change the IP address associated with an alias host name.

Some cluster systems make shared storage available or writable to only one computer at a time. This is not suitable for some CA Workload Automation AE components. The $AUTOSYS directory may be read-only after installation. Other directories must be writable for each component.

Each persistent CA Workload Automation AE process comes with a script to start it at startup, if appropriate. The cluster systems can use the same scripts to control the CA Workload Automation AE processes.

Cluster Configuration Options

This section explains the options you can use when configuring CA Workload Automation AE components in a cluster.

Application Server

The CA Workload Automation AE application server can operate in either passive-active mode, in which only one copy runs at a time, or in active-active mode, in which a copy runs concurrently on more than one computer. The cluster system can use the active-active mode for load balancing. In either mode, the clients and schedulers must refer to the application server using a movable host name.

The CA Workload Automation AE application server writes log files in the $AUTOUSER/out directory.

Scheduler

The CA Workload Automation AE scheduler can operate only in passive-active mode. Only one copy can run at a time. There is no need to associate a movable host name with the scheduler. No other CA Workload Automation AE component initiates contact with the scheduler.

Do not use the CA Workload Automation AE scheduler's built-in high availability features when operating it under the control of a cluster system.

Remember to use the movable host name for the application server when configuring the scheduler. The scheduler passes the application server's host name to the agent when running jobs.

The CA Workload Automation AE scheduler writes log files in the $AUTOUSER/out directory. It runs nightly maintenance jobs which writes files in the $AUTOUSER/archive directory.

Agent

The CA Workload Automation AE agent operates in active-active mode. It is not necessary to place the agent under the control of the cluster system.

Client

Remember to use the movable host name for the application server when configuring CA Workload Automation AE clients.

Cluster Control Scripts

The application server, scheduler, and agent control scripts reside in the usual directory appropriate for the platform. You may copy the scripts to another location if you want them to be uniform in a mixed-vendor environment.

Operating System	Script Directory
AIX	/etc/rc.d/
HP-UX	/sbin/init.d/
Linux and Solaris (SunOS)	/etc/init.d/

The CA Workload Automation AE components and their script files are as follows:

Component	Script File
Agent	waae_agent-*WA_AGENT*

Component	Script File
Application Server	waae_server.$AUTOSERV
Scheduler	waae_sched.$AUTOSERV

Each script accepts one of the commands in the following table as its only argument:

Command	Purpose	Exit Status
start	Starts the component.	0 on success, 1 on failure
stop	Stops the component.	0 on success, 1 on failure
status	Reports the component status.	0 if running, 1 if not running
monitor	Reports status of veritas.	110 if running, 100 if not running

For example, the following script starts the CA Workload Automation AE application server for instance ACE on a Linux computer:

```
/etc/init.d/waae_server.ACE start
```

You can enter this string in your cluster configuration when preparing to run the application server under the control of the cluster system. Enter the stop and status or monitor commands similarly.

If you place the CA Workload Automation AE components under the control of the cluster system, do not start those components independently at startup.

Defining Jobs within a Cluster System

The CA Workload Automation AE agent answers to any working host name for the computer on which it is running. This lets CA Workload Automation AE jobs cooperate with the cluster system when resources other than CA Workload Automation AE itself migrate from one computer to another.

For example, the cluster system can run an application named BigApp on either a computer named colossal or a computer named mammoth. Suppose the job big_job must run on the computer that is currently running the application BigApp. The cluster system can be configured to associate a movable host name, such as a computer named giant with the application BigApp, and use the computer named giant in the definition of the job big_job.

Shared Storage in a Cluster System

CA Workload Automation AE does not require shared storage for proper operation in a cluster. If you have shared storage in your cluster, you can use it for CA Workload Automation AE in the following cases:

- The $AUTOUSER directory must be writable by the scheduler, the application server, and the archive_events command. If you place the scheduler and the application server under the control of your cluster system, you can select to place $AUTOUSER in shared storage, which is writable where they are running. Sharing $AUTOUSER lets the scheduler and application server log files remain in the same place when the cluster system changes the computer on which the programs are running.
- The $AUTOSYS directory need not be writable after installation. You may place it in shared storage as long as it remains readable by all agents at all times. However, it is probably more convenient to keep a private copy on each computer.

Implementing CA Workload Automation AE and CA WCC

When you implement CA Workload Automation AE and CA WCC, we recommend that you install the CA products in the following order:

- CA EEM

  Note: CA EEM is optional for CA Workload Automation AE; however, it is required for CA WCC. We recommend that you configure CA Workload Automation AE to use CA EEM for enhanced security. CA EEM is installed using the CA Common Components DVD and must be installed and running before you install CA Workload Automation AE or CA WCC.

- CA Workload Automation AE components

  Note: When you install CA Workload Automation AE, the Command Sponsor is installed. The Command Sponsor lets you execute CA Workload Automation AE commands (such as autorep, chk_auto_up, autoping, and so on) on the CA Workload Automation AE server using the CA WCC user interface.

- CA WCC
- CA Workload Automation agents
- Required patches for CA Workload Automation AE, CA WCC, and the agents

Notes:

- For information about installing CA EEM, see the *CA Common Components Implementation Guide*.
- For information about installing CA WCC, see the CA WCC *Implementation Guide*.
- We recommend that you install all operating system patches before installing any of the CA products. For CA patch information, see the *CA Common Components Readme*, the CA Workload Automation AE *Readme*, and the CA WCC *Readme*. The CA patches are available from the CA Support web page (http://ca.com/support).

Product DVDs and Installation Files

You must run several installation files to set up CA Workload Automation AE and CA WCC in a typical environment.

The following table describes the DVDs, installation files, and the guides to refer to when installing the CA products:

CA Product	DVD to Use	Installation File	Guide to Refer to
CA Common Components	CA Common Components DVD **Note:** You can install the following components using the CA Common Components DVD: ■ CA EEM ■ SSA ■ Event Management ■ CAICCI ■ Management Command Center **Note:** On Windows, you cannot install Management Command Center using the CA Common Components DVD.	ccc_setup.sh (on UNIX) setup.exe (on Windows)	*CA Common Components Implementation Guide*
CA Workload Automation AE	CA Workload Automation AE DVD	wa_setup.sh (on UNIX) setup.exe (on Windows)	*UNIX Implementation Guide* *Windows Implementation Guide*
CA WCC	CA WCC DVD	UnixInstaller.sh (on UNIX) PE_i386.EXE (on Windows)	*CA WCC Implementation Guide*

CA Product	DVD to Use	Installation File	Guide to Refer to
CA Workload Automation Agent for UNIX, Linux, or Windows	CA Workload Automation AE DVD **Note:** You can also install the agent using the CA Workload Automation Agent for UNIX, Linux, or Windows DVD. However, we do not recommend it. For more information about installing the agent using the CA Workload Automation Agent for UNIX, Linux, or Windows DVD, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.*	wa_setup.sh or agent_setup.sh (on UNIX) setup.exe (on Windows)	*UNIX Implementation Guide* *Windows Implementation Guide*
Agent plug-ins	CA Workload Automation Agent for UNIX, Linux, or Windows DVD	agent plug-in installation files	*Implementation Guide* for the appropriate agent plug-in

How to Implement CA Workload Automation AE and CA WCC

The following table lists the basic tasks you must perform to set up CA Workload Automation AE and CA WCC in a typical environment.

Notes:

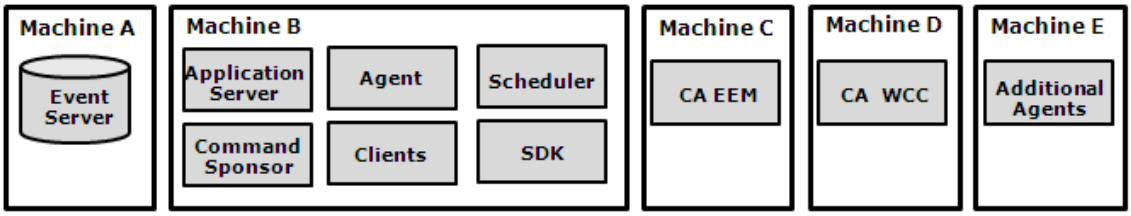
- You can perform the tasks listed in the table if you are installing CA Workload Automation AE for the first time or installing CA Workload Automation AE in a test environment before upgrading and migrating your data to the current release.
- We recommend that you install the CA products in the order listed in the table.

Installation Phase	Tasks to Perform
Pre-Installation	Plan your environment (see page 36)
	Get the required CA Workload Automation AE licenses (see page 36)
	Set up the database for CA Workload Automation AE (see page 37)
Installation	Install CA EEM (see page 37)

Installation Phase	Tasks to Perform
	Install and verify the CA Workload Automation AE server (see page 38) **Note:** Before you install CA Workload Automation AE, you must ensure that the system requirements are met on the server computer. For more information about the system requirements, see the *CA Workload Automation AE Release Notes*. For information about the considerations you must review when you install CA Workload Automation AE, see the following topics: ■ Mount the DVD-ROM Device (see page 55) ■ Mounting the DVD on HP-UX (see page 55). ■ Installation Considerations (see page 57)
	Install, configure, and verify CA WCC (see page 38)
	Install and verify additional agents on other computers (see page 39)
	Install and verify agent plug-ins (see page 39)
Post-Installation	Install the required patches (see page 39)
	Set up custom CA EEM security policies (see page 40)

Plan Your Environment

Before you install the CA products, you must identify the computers on which you want to install the CA products, and decide which CA product to install on each computer. We recommend that you install the CA Workload Automation AE components, CA EEM, CA WCC, and additional agents on separate computers as follows:



Note: For more information about identifying the computers to install the CA Workload Automation AE components, see Identify Computers (see page 50).

Get the Required CA Workload Automation AE Licenses

After you install CA Workload Automation AE, you must apply the scheduler and agent licenses. For more information about getting and applying licenses, contact Technical Support at http://ca.com/support.

Note: For more information about the required licenses for CA Workload Automation AE, see Required Licenses (see page 69).

Set Up the Database for CA Workload Automation AE

Ask your database administrator to set up the database (event server) for CA Workload Automation AE. Record the database administrator password. You need this information during the CA Workload Automation AE installation.

Note: For more information about the considerations you must review before setting up the CA Workload Automation AE database, see the following topics:

- Database-specific Environment Variables (see page 43)
- Host Machine Checklist (see page 51)
- Installing into an Existing MDB (Oracle Only) (see page 58)
- Installing CA Workload Automation AE with Sybase (see page 58)
- Installing CA Workload Automation AE with Oracle (see page 60)
- Installing CA Workload Automation AE with Oracle 10g (see page 61)
- Configure the Environment to Use a 64-bit Database (see page 63)

Install CA EEM

You can install CA EEM using the CA Common Components DVD. CA EEM is optional for CA Workload Automation AE; however, it is required for CA WCC. We recommend that you configure CA Workload Automation AE to use CA EEM for enhanced security.

CA EEM must be installed and running before you install CA WCC or CA Workload Automation AE (if you are using CA EEM security). Record the CA EEM password. You need this information during the CA Workload Automation AE and CA WCC installation.

Notes:

- For information about configuring CA Workload Automation AE or CA WCC to work with CA EEM, see the *CA Workload Automation Security Guide*.
- For more information about installing CA EEM, see the CA Common Components documentation.

Install and Verify the CA Workload Automation AE Server

You can install the CA Workload Automation AE server using the CA Workload Automation AE DVD. If you perform a custom installation, we recommend that you select all the components.

Notes:

- When you install CA Workload Automation AE, ensure that you install the Command Sponsor component. The Command Sponsor lets you execute CA Workload Automation AE commands (such as autorep, chk_auto_up, autoping, and so on) on the CA Workload Automation AE server using the CA WCC user interface.
- During the CA Workload Automation AE installation, select the option to create the CA EEM security policies for the CA Workload Automation AE instance. CA Workload Automation AE is registered with CA EEM and the default security policies are created. If you select to create the CA EEM security policies for the CA Workload Automation AE instance, you must have CA EEM installed locally or on a remote host.
- After you install CA Workload Automation AE, we recommend that you use the CA EEM web interface to customize the default security policies or create new security policies and grant access modes based on your requirements.
- For more information about installing the CA Workload Automation AE server, see Installing the Server (see page 67).
- You can verify the CA Workload Automation AE server installation by running a test job. For more information, see Running a Test Job (see page 93).

Install, Configure, and Verify CA WCC

You can install CA WCC using the CA WCC DVD.

Notes:

- Before you install CA WCC, you must install the CA Workload Automation AE SDK on the CA WCC server using the CA WCC DVD. For information about installing the CA Workload Automation AE SDK and CA WCC, see the *CA Workload Control Center Implementation Guide* and the *CA Workload Control Center Release Notes*.
- After you install CA WCC, you must configure CA WCC to work with CA EEM and define your CA Workload Automation AE servers in CA WCC. For information about security policies and how to create them in CA EEM, see the *CA Workload Automation Security Guide*. For information about configuring CA WCC, see the *CA Workload Control Center Implementation Guide*.
- You can verify that CA WCC works with CA Workload Automation AE by creating a job using the CA WCC Quick Edit application. You can monitor the job using the CA WCC Job Status Console application. For information about creating a job, see the *CA Workload Control Center Quick Edit Help*. For information about monitoring a job, see the *CA Workload Control Center Job Status Console Help*.

Install and Verify Additional Agents on Other Computers

You can install additional agents on other computers (other than the CA Workload Automation AE server or client computers) using the CA Workload Automation AE DVD.

Notes:

- You can use the wa_setup.sh or agent_setup.sh script to install additional agents on other computers. For more information about using the wa_setup.sh or agent_setup.sh script to install additional agents on other computers, see Installation Scenarios (see page 108).
- You can also install the agent using the CA Workload Automation Agent for UNIX, Linux, or Windows DVD. However, we do not recommend it. If you install the agent using the CA Workload Automation Agent for UNIX, Linux, or Windows DVD, you must configure it to work with CA Workload Automation AE. For more information about installing the agent using the CA Workload Automation Agent for UNIX, Linux, or Windows DVD and configuring it to work with CA Workload Automation AE, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide*.
- If you install the agent using the CA Workload Automation AE DVD, the agent is configured specifically for use with CA Workload Automation AE. For more information about installing the agent, see Installing the Agent (see page 107). For information about configuring the agent to work with CA Workload Automation AE, see Configuring CA Workload Automation AE to Work with the Agent (see page 163).

Install and Verify Agent Plug-ins

You can use the agent plug-in installation files located on the CA Workload Automation Agent for UNIX, Linux, or Windows DVD to install the agent plug-ins.

Note: For more information about installing the agent plug-ins, see the *Implementation Guide* and *Release Notes* for the appropriate agent plug-in.

Install the Required Patches

You must install the patches for CA Workload Automation AE, CA WCC, agents, and common components.

Note: For information about the patches, see the *CA Common Components Readme*, the CA Workload Automation AE *Readme*, the CA WCC *Readme,* and the *CA Workload Automation Agent for UNIX, Linux, or Windows Readme.* The patches are available from the CA Support web page (http://ca.com/support).

Set Up Custom CA EEM Security Policies

After you install and verify CA EEM, CA Workload Automation AE, and CA WCC, you can customize the default security policies or create new security policies and grant access modes based on your requirements.

Note: For more information about the security policies and how to create them in CA EEM, see the *CA Workload Automation Security Guide*.

Chapter 2: Environment and Database Connection

This section contains the following topics:

Environment

Access to CA Workload Automation AE is controlled by environment variables and configuration parameters, which must be set for the product to run properly. The installation process creates files that are sourced when the user logs on.

All processes must know the following:

- Which databases to connect to for reading events and definitions.
- Which directories to access for writing output files.

Environment Variables

CA Workload Automation AE consults the following environment variables to run properly and to determine which instance to connect to:

AUTOSYS

Identifies the full path to the CA Workload Automation AE installation directory.

AUTOUSER

Identifies the directory containing instance-wide configuration files, scheduler or application server output files, encryption files, archive output files generated during database maintenance, and sound files (for operating environments supporting audio functionality).

AUTOSERV

Identifies the unique, uppercase three-letter name of a CA Workload Automation AE instance.

To communicate with the Sybase or Oracle database, CA Workload Automation AE also relies on the environment variables. If only one instance is running, the environment variables can be set during login by including their definitions in either the .profile or .cshrc file for each user accessing CA Workload Automation AE.

The installation script generates files that are designed to be sourced by a user wanting to access CA Workload Automation AE. The following files can be sourced from a .profile or .cshrc file and are found in the $AUTOUSER directory:

- autosys.sh.*hostname*—for Bourne shell users
- autosys.csh.*hostname*—for C shell users
- autosys.ksh.*hostname*—for Korn shell users
- autosys.bash.*hostname*—for Bash shell users

Optionally, frequently used variations for the sendevent, autorep, and eventor commands can be aliased in the files to be sourced.

Note: For more information about these commands, see the *Reference Guide*.

Configuration Parameters

You can define the CA Workload Automation AE environment using configuration parameters. The configuration parameters include information about the agents, event servers, scheduler, application servers, and many tunable parameters that control the behavior of CA Workload Automation AE.

Some configuration parameters are defined when you install CA Workload Automation AE and the rest have default settings. You need not modify these settings if the installation specifications are acceptable.

Note: Properly setting the required environment variables in every user's environment and configuring CA Workload Automation AE correctly helps to prevent potential problems. The most common problems are that CA Workload Automation AE cannot determine which event server to connect to and it cannot locate various executables or files.

/etc/auto.profile File

The /etc/auto.profile file is one of the several objects that source the environment for a job. The /etc/auto.profile file is automatically created during installation and contains variable definitions such as AUTOUSER. The file is located on the computer where CA Workload Automation AE is installed.

System environment variables are automatically set in the environment for a job. When a job is submitted, the agent processes the following additional information to source the environment, in the following order:

1. /etc/auto.profile
2. Environment variables defined using the envvars attribute in the job definition (if specified)
3. The job profile defined using the profile attribute (if specified)

Note: For more information about the envvars and profile attributes, see the *Reference Guide*. For more information about how job profiles work, see the *User Guide*.

Database-specific Environment Variables

CA Workload Automation AE uses database-specific environment variables and configuration settings to locate and connect to the database (that is, the event server).

Oracle

If you are using an Oracle database, SQL*Net V2 must be installed and configured correctly on the machine on which you will be installing a CA Workload Automation AE scheduler or application server. In particular, the TNS alias name of the data server that CA Workload Automation AE uses must be configured, and an SQL*Net V2 connect descriptor must be in the TNS names configuration file.

The tnsnames.ora file is used by CA Workload Automation AE to look for the database host computer and port number based on the event server name. It is the means by which the network is navigated to find the Oracle data server. This file specifies where the Oracle server is located. The tnsnames.ora file is usually in the $ORACLE_HOME/network/admin or $TNS_ADMIN directory.

Sybase

If you are using a Sybase data server, the following environment variables are used:

DSQUERY

Defines the name of the Sybase data server.

SYBASE

Identifies the complete path to the Sybase software directory.

The Sybase software directory contains the Sybase configuration file, which is the interfaces file. CA Workload Automation AE uses the Sybase configuration file to look for database information.

Note: We recommend that you set the SYBASE environment variable before running the wa_setup.sh script. By doing so, the appropriate default database values will be provided during installation.

Database Connection

All information is stored in a Relational Database Management System (RDBMS) called the event server, which is configured for CA Workload Automation AE. Access to CA Workload Automation AE requires a connection to this database, that is, you must connect to the database to add, modify, control, report on, or monitor jobs, and to change certain configuration settings.

The configuration parameters and the database environment variables (described previously) tell the software which databases to connect to for a particular instance.

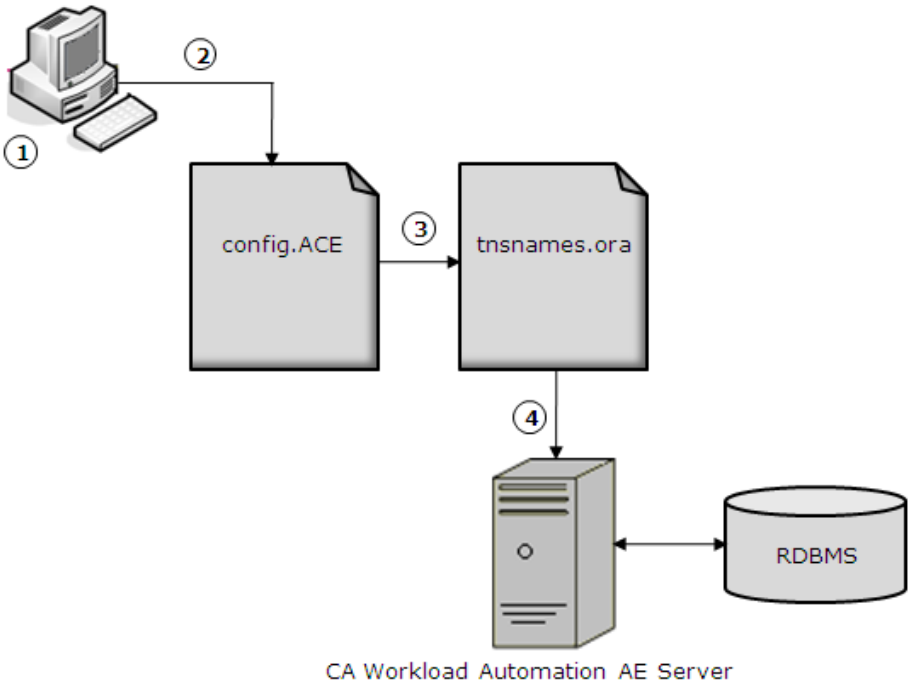
More information:

How CA Workload Automation AE Connects to an Oracle Database (see page 45)
How CA Workload Automation AE Connects to a Sybase Database (see page 46)

How CA Workload Automation AE Connects to an Oracle Database

The following illustration and explanation describe how CA Workload Automation AE connects to an Oracle database:

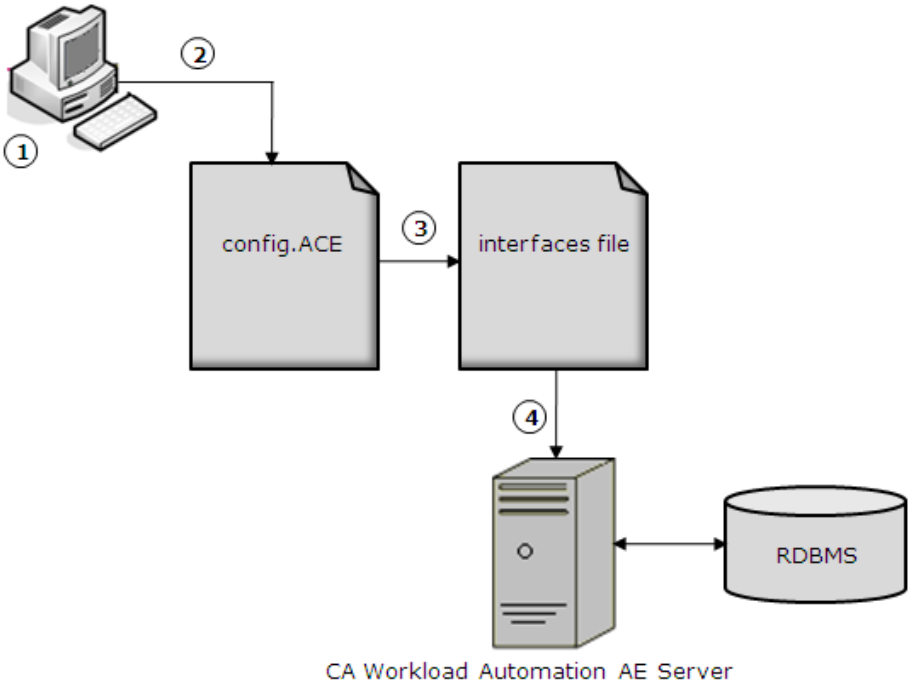
1. Reads the $AUTOUSER/config.$AUTOSERV file and locates the event server and database configuration settings. For example: EventServer=MYORACLEDB.
2. Searches for the TNS alias MYORACLEDB in the tnsnames.ora file.
3. Uses network configuration information to connect to SQL* Net V2 and the Oracle database.



How CA Workload Automation AE Connects to a Sybase Database

The following illustration and explanation describe how CA Workload Automation AE connects to a Sybase database:

1. Reads the $AUTOUSER/config.$AUTOSERV file and locates the event server and database configuration settings. For example: EventServer=AUTOSYSDB:autosys.
2. Searches for AUTOSYSDB in the interfaces file.
3. Uses the host name and port number entry to connect to the database.



Chapter 3: Installation Preparation

This section contains the following topics:

Before You Begin

The CA Workload Automation AE installation automates the process of installing and configuring CA Workload Automation AE software. Some of the steps in the installation procedures may not be necessary for all configurations.

Note: Before proceeding with the CA Workload Automation AE installation, verify the existence of a valid TMPDIR environmental variable that refers to a valid directory on the installation computer. The /tmp directory is used if $TMPDIR is not set.

The setup program creates a log file in the /opt/CA/installer/log directory called CAWorkloadAutomationAE.install.log. This file contains a summary of the components installed. Refer to this file if you encounter problems during installation.

If the installation fails, the installation log is created in the $TMPDIR or /tmp directory.

System Requirements

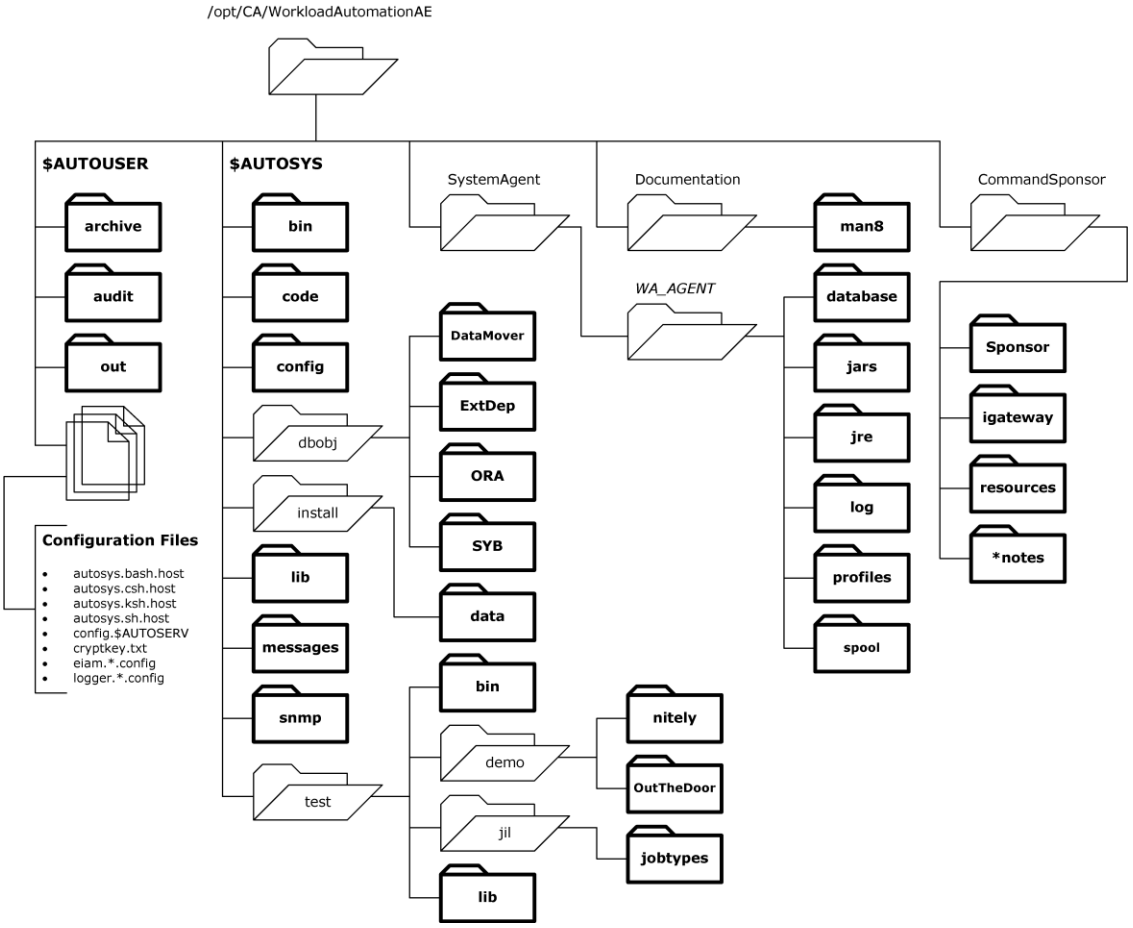
For information about system requirements, see the *Release Notes.*

Notes:

- For current information regarding platform support, check the CA Workload Automation Support web page at http://ca.com/support.
- For information about CA Common Components system requirements, operating system support, and installation considerations, see the *CA Common Components Release Notes*.

Directory Structure

The following illustration shows the default directory structure for CA Workload Automation AE with /opt/CA/WorkloadAutomationAE as the installation directory. The $AUTOUSER directory can be placed elsewhere. The location for new directories is pointed to by the AUTOSYS and AUTOUSER environment variables.



Changes to System Files and Directories

The following changes are made to the existing system files and directories during the installation. Unless noted, these changes are made on all installed computers:

- The auto.profile file is created in the /etc directory.
- The startup scripts CA-CCS, CA-WAAE, waae_agent-*, waae_sched.*, and waae_server.* are created in the appropriate directories: /etc/init.d, /etc/rc.d, or /sbin/init.d.
- The installer creates a directory to store control files. By default, the /opt/CA/installer directory is created. The installer stores files in /opt/CA/installer. A link is created from /var/sdadm to /opt/CA/installer. A link to lsm is created in /usr/bin.

  Note: If no other CA products are installed on the machine, and if you want to use another directory besides /opt/CA, you must set the environment variable CASHCOMP. For example, you will need another directory if /opt is a read-only file system. To have the installer use /local/CA, run the following commands:

  ```
  CASHCOMP=/local/CA
  export CASHCOMP
  ./wa_setup.sh
  ```

  The installer directory must have at least 10 MB of free space.
- By default, the CA Workload Automation AE installer updates the following files, depending on the platform you are using:
  - /etc/profile and /etc/csh.login (on Linux)
  - /etc/profile and /etc/.login (on Sun Solaris)
  - /etc/profile and /etc/csh.login (on IBM AIX)
  - /etc/profile and /etc/csh.login (on HP-UX)

  Note: To override this default during installation, you must clear the Profile Update check box on the Installation Type page.

Components to Install

You can use the setup program to install different combinations of components on various computers, and also to install these components for each instance that you want to run. A custom installation provides greater flexibility in component selection, while a typical installation automatically selects all applicable product components. You must run the setup program on each computer on which you install a CA Workload Automation AE component.

The following components are available for installation:

Scheduler

Interprets CA Workload Automation AE events and, based on job definitions, initiates actions through the agent.

Application Server

Enables programs to securely access the database without installing a database client.

Agent

Performs tasks such as running jobs and reporting their status.

Client

Lets you define, run, and maintain all CA Workload Automation AE instances and jobs.

SDK

Provides the necessary tools to build your own applications to manipulate product data.

Documentation

Installs the product documentation.

Command Sponsor

Lets you execute JIL commands on a CA Workload Automation AE server using the CA WCC user interface.

Identify Computers

Before you install CA Workload Automation AE, identify the computers on which you want to install the required components, and decide which components to install on each computer.

Server Computers

The *server* is a computer on which the database, the scheduler, or both reside.

You should identify at least one computer on which to install the database. To ensure high availability of the database, you can install dual event servers; in that case, you need two computers on which to install databases.

Note: The terms *event server* and *database* are often used interchangeably.

You can also install a shadow scheduler to ensure high availability of the scheduler. This requires two additional computers: a shadow computer and a tie-breaker computer. The primary, shadow, and tie-breaker computers must all be of the same type, either Windows or UNIX. All three computers must be defined in the same instance.

Host Machine Checklist

Use the following table to collect information about your host machine:

Information	Your Selection or Value
Platform	
Operating system/version	
Host name	
Password of root	
Minimum requirements—Available memory (1 GB)	
Minimum requirements—Available disk space (1 GB)	
Name of data server that contains the database	
(Oracle only) The location of the Oracle tnsnames.ora file	
(Sybase only) The location of the Sybase interfaces file	
Password for database user who has been granted DBA role	

Note: For information about system requirements, see the *Release Notes*.

Client and Agent Computers

You should identify one or more computers on which to install the client, the agent, or both. You can define an agent computer to run jobs only, or a client computer to run both the jobs and the client utilities that let you define and monitor jobs.

Computers that Require CAICCI

CA, Inc. Common Communications Interface (CAICCI) is a transport layer that lets CA Workload Automation AE communicate with mainframe products such as CA Workload Automation SE in a legacy capacity and legacy-based agents on AS/400 (i5/OS) and OpenVMS. You should identify the computers on which you want to integrate CA Workload Automation AE with these legacy solutions.

Note: For information about configuring your computers for CAICCI, see the *CA Common Components Implementation Guide*.

Install JRE

On AIX, you must install JRE before installing CA Workload Automation AE. The installation program prompts you for the full path to the JRE directory and the java binary located in the JRE directory.

Notes:

- For information about the JRE version to be installed, see the *Release Notes*.
- The supported JRE is 32-bit. The 64-bit JRE is not supported.

How to Customize the CA Workload Automation AE Installation

You can customize the CA Workload Automation AE installation by setting the operating system environment variables to perform the following tasks:

- Enable tracing (see page 53)
- Modify the Sybase character set (see page 54)
- Disable disk space check (see page 54)
- Disable source database connection check (see page 55)

Enable Tracing

By default, high-level tracing is enabled during the CA Workload Automation AE installation, logging basic troubleshooting information. The tracing information is written to the following three files in the /tmp directory:

- as_install<pid>.trc–The panel name trace file.
- as_install<pid>.tvars–The trace file that includes the environment variables at the time of each panel is displayed.
- as_install<pid>.vars–The trace file that includes the environment variables at the time of the installation.

To enable tracing only in the installation prestart process, run the following command:

```
WA_DEBUG=1; export WA_DEBUG
```

The trace information is written to standard output.

To enable tracing only in the CA Workload Automation AE database creation process on Oracle or Sybase, run the following command:

```
WA_DB_DEBUG=1; export WA_DB_DEBUG
```

Note: You can disable high-level tracing. However, we recommend that you enable tracing. It helps you debug installation problems.

To disable tracing, run the following command:

```
AS_INSTALL_DEBUG=0; export AS_INSTALL_DEBUG
```

To enable low-level tracing, specify the –t option when you run the wa_setup.sh script.

More Information:

wa_setup.sh—Install, Update, or Remove CA Workload Automation AE (see page 87)

Modify the Sybase Character Set

If you are using the Sybase data server, the following environment variable identifies the Sybase character set used during the CA Workload Automation AE installation:

```
AS_SYB_LOCALE=iso_1
```

You can modify the Sybase character set used during the CA Workload Automation AE installation.

To modify the Sybase character set during the CA Workload Automation AE installation, set the AS_SYB_LOCALE environment variable as follows:

AS_SYB_LOCALE=*value*

value

Specifies the value of the AS_SYB_LOCALE environment variable. The default value is iso_1.

When CA Workload Automation AE connects to the Sybase server, the character set is set to the specified value.

Notes:

- If you modify the CA Workload Automation AE installation or re-install CA Workload Automation AE, you can modify the Sybase character set by editing the /tmp/as_syb_locale file. For example, to set the character set to ISO_8859-2, run the following command:

  ```
  echo iso88592 > /tmp/as_syb_locale
  ```

- For more information about the Sybase locales and character sets, see the Sybase documentation.

Disable Disk Space Check

The CA Workload Automation AE agent installation requires 260 MB of available temporary space.

To disable the disc space check, run the following command:

```
AS_SKIP_SPACE_CHECK=1; export AS_SKIP_SPACE_CHECK
```

Note: If you modify the CA Workload Automation AE installation or re-install CA Workload Automation AE, you can disable the disc space check by creating the /tmp/as_skip_space_check file. To create this file, run the following command:

```
touch /tmp/as_skip_space_check
```

Disable Source Database Connection Check

When you migrate data from Unicenter AutoSys JM 4.5 or r11 to CA Workload Automation AE r11.3, a check is made to verify whether the source database can be connected to. You can disable this source database connection check in certain situations, for example, when the database is temporarily unavailable.

To disable the source database connection check, run the following command:

```
AS_MIG_VERIFY=no; export AS_MIG_VERIFY
```

Note: If you modify the CA Workload Automation AE installation or re-install CA Workload Automation AE, you can disable the source database connection check by creating the /tmp/as_mig_verify file. To create this file, run the following command:

```
touch /tmp/as_mig_verify
```

Mount the DVD-ROM Device

Before you begin the installation or upgrade to CA Workload Automation AE r11.3, you must mount the DVD-ROM device on the UNIX computer.

To mount the DVD-ROM device

1. Create the /cdrom directory (if it does not exist) using the following command:

   ```
   # mkdir /cdrom
   ```

2. Mount the DVD-ROM drive using the mount command.

Mounting the DVD on HP-UX

When mounting the DVD on HP-UX, you must use the Rock Ridge extension to the ISO-9660 file system. Review the man page for the appropriate mount command.

Example of a mount command:

```
mount -o rr /cdrom
```

Chapter 4: Installation Considerations

The following sections provide information related to the installation of CA Workload Automation AE.

Notes:

- For more information about the supported operating systems, supported databases, required third-party patches, and system requirements, see the *Release Notes*.
- For more information about issues known to exist in this version, see the *Readme*.

This section contains the following topics:

Installing CAICCI

Consider the following when installing CAICCI (CA, Inc. Common Communications Interface) on UNIX or Linux:

- CA Workload Automation AE supports CAICCI r11.2. If you use an existing CAICCI r11.2 instead of installing it from the CA Common Components DVD, do not uninstall the application that initially installed CAICCI. Doing so can result in CA Workload Automation AE being adversely impacted because CAICCI is also uninstalled.
- On UNIX/Linux, the user definitions of previous releases of CAICCI are stored in ccirmtd.prf, located at $CAIGLBL0000/cci/config/<hostname>. When you install CA Workload Automation AE r11.3, CAICCI is installed in $CASHCOMP/ccs/cci. You must move the ccirmtd.prf from $CAIGLBL0000/cci/config/<hostname> to $CASHCOMP/ccs/cci/config/<hostname> to use your existing CAICCI configuration. Later, if you reinstall the ca-cs-cci package over an already installed instance of the same or lower version, all the files are replaced with the new ones.

Installing CA EEM

To administer the CA Workload Automation AE user-defined policies, you must use the CA EEM web server.

Reinstalling CA Workload Automation AE

Before reinstalling CA Workload Automation AE on UNIX or Linux to add or remove features, you must stop all CA Workload Automation AE processes. You can issue the following commands using the root account:

```
unisrvcntr stop CA-WAAE
$CSAM_SOCKADAPTER/bin/csampmux stop
```

Installing into an Existing MDB (Oracle Only)

If you are using Oracle, you can install CA Workload Automation AE into the same SID that contains a database from a previous release of CA Workload Automation AE. The MDB is updated as follows:

- Separate tablespaces are created for the new CA Workload Automation AE instance.
- The new tables and stored procedures are added under the aedbadmin user.
- The global synonyms (send_event, alamode, event, intcodes, proc_event, and timezones) for the new instance replace the previous definitions. This is because a global synonym in an SID can only have one definition.

Note: On Sybase and Microsoft SQL Server, installing CA Workload Automation AE into an existing MDB is not supported. You must create a new database.

Installing CA Workload Automation AE with Sybase

Consider the following when installing CA Workload Automation AE r11.3 with Sybase:

LANG Variable

Before installing CA Workload Automation AE on UNIX, check the LANG environment variable on your system. The LANG environment variable value on the session that the CA Workload Automation AE installation was launched must match the value of the LANG environment variable on the session from which Sybase was started.

To display the LANG environment variable, run the following command from both the CA Workload Automation AE session and the session from which Sybase was started:

```
echo $LANG
```

If they are different, change the LANG value to match the value on the Sybase session by running the following command from the CA Workload Automation AE session:

```
LANG=value; export LANG
```

User Connections

Before installing CA Workload Automation AE, you must set the Sybase available user connections as appropriate. CA Workload Automation AE requires up to 115 free Sybase user connections, depending on which components you install. The following list states the number of Sybase user connections required for each component of CA Workload Automation AE:

- Scheduler: 16+4
- Application Server: 35
- High Availability (2 Schedulers and 2 Application Servers): 110
- Tie-breaker Scheduler: 5

For example, a typical CA Workload Automation AE server installation with High Availability requires 115 Sybase user connections. When determining the minimum number of user connections required to support your configuration, you must account for the user connections used by Sybase itself, typically about 15 for each machine. The number may vary depending upon the version of Sybase. Thus, if CA Workload Automation AE is the only Sybase application in a typical High Availability environment, the minimum number of user connections needed would be calculated as follows: (2 Schedulers x 20) + (2 Application Servers x 35) + (1 Tie-breaker Scheduler x 5) + (3 machines x 15) = 150.

Run the following SQL command to determine the number of configured user connections:

```
1>sp_configure 'user connections'
2>go
```

Run the following SQL command to determine the number of user connections currently in use:

```
1>sp_who
2>go
```

The number of rows returned from the above command represent the number of user connections currently in use. This number can be subtracted from the configured amount to determine the number of free user connections.

Run the following SQL command to set the number of user connections to 64:

```
1>sp_configure 'user connections', 64
2>go
```

Page Size

The default Sybase installation comes with a page size of 2 KB. However, CA Workload Automation AE requires the minimum page size to be at least 4 KB. Enter the following command to check the current page size:

```
select @@maxpagesize
```

Note: For information about changing the page size, see the Sybase documentation.

Runtime Configuration

CA Workload Automation AE uses the Open Client/Open Server interface with Sybase. If your Sybase environment uses the runtime configuration file (ocs.cfg) and Sybase Open Client/Open Server products are used in your Sybase environment, you must update ocs.cfg with the corresponding application sections. Add the following information to ocs.cfg, located at $SYBASE/$SYBASE_OCS/config (UNIX) or %SYBASE%\%SYBASE_OCS%\ini (Windows), before starting the CA Workload Automation AE processes:

```
[CA WAAE Application Server]
    CS_SEC_ENCRYPTION = CS_TRUE

[CA WAAE Scheduler]
    CS_SEC_ENCRYPTION = CS_TRUE
```

Installing CA Workload Automation AE with Oracle

Consider the following when installing CA Workload Automation AE r11.3 with Oracle:

Defining an Oracle User to Run CA Workload Automation AE

When installing Oracle AEDB and creating tablespaces and users, the CA Workload Automation AE installer must connect to the Oracle database with an Oracle user created with sufficient authority. The following SQL statements let you define an Oracle user with authority to run CA Workload Automation AE:

```
CREATE USER <user> IDENTIFIED BY <password>;
GRANT DBA TO <user>;
GRANT CREATE SESSION TO <user>;
GRANT SELECT ON "SYS"."DBA_TABLESPACES" TO <user> WITH GRANT OPTION;
```

Installing CA Workload Automation AE with Oracle 10g

Consider the following when installing CA Workload Automation AE r11.3 with Oracle 10g on UNIX or Linux:

Oracle 10g Directory Permissions

CA Workload Automation AE requires access to the Oracle shared libraries. Oracle 10g, by default, does not allow this access. You must perform one of the following procedures for CA Workload Automation AE to function properly:

- Before running the CA Workload Automation AE installation, create the autosys OS user and specify Oracle's OSDBA group as the autosys primary group, or add Oracle's OSDBA group to the autosys supplemental group list.
- Allow the CA Workload Automation AE installation to automatically create the autosys OS user. When you are prompted to specify the autosys owner and group, specify Oracle's OSDBA group as the autosys group.

If one of these two procedures is not followed, the CA Workload Automation AE startup will fail with the following message:

```
CAUAJM_E_90013 Unable to load Oracle client libraries
</opt/CA/CAlib/libclntsh.so: cannot open shared object file: No such file or
directory>
CAUAJM_E_10368 Failed to connect to Oracle server: <SID>
Cannot find key="" in the resource bundle
CAUAJM_E_10649 Server orcl was not available during connection operation.
```

Determine the OSDBA group

To determine the OSDBA group, issue the following command:

```
ls -dl $ORACLE_HOME | awk '{print $4}'
```

Modify an Existing autosys User

To add the owner of an existing autosys user to the OSDBA group, issue the following command. For this example, the OSDBA group is dba and the autosys owner is autosys.

HP-UX, Linux, Solaris:

```
usermod -G dba autosys # To add to the supplemental group list
usermod -g dba autosys  # To set as the primary group
```

AIX:

```
chuser groups=dba autosys # To add to the supplemental group list
chuser pgrp=dba autosys # To set as the primary group
```

Create the autosys User

To create the autosys user and set its primary or supplemental group as the OSDBA group, issue the following command:

HP-UX, Linux, Solaris:

```
useradd -G dba autosys  # To add to the supplemental group list
useradd -g dba autosys  # To set as the primary group
```

AIX:

```
mkuser groups=dba autosys # To add to the supplemental group list
mkuser pgrp=dba autosys # To set as the primary group
```

Using Oracle Instant Client

If an Oracle user decides to use the Oracle Instant Client instead of a native Oracle client, the following modifications must be made to the base Oracle Instant Client installation:

- Oracle Instant Client users must set up a directory structure that looks exactly like a native Oracle client installation.
- The shared libraries must reside in ORACLE_HOME/lib directory and the sqlplus binary must reside in ORACLE_HOME/bin directory. In addition, the user must create a soft link for libclntsh in the ORACLE_HOME/lib directory.

Configure the Environment to Use a 64-bit Database

To use CA Workload Automation AE with the 64-bit version of Oracle or Sybase, you must install the 32-bit client if it is not already installed. Do this procedure before you install CA Workload Automation AE.

Notes:

- Releases of Oracle prior to 11g Release 2 installed with a lib32 directory that contained the required 32-bit libraries. You can skip this procedure if the 32-bit libraries are already installed. On Oracle 11g Release 2 and later, the 64-bit installation no longer creates the lib32 directory. Therefore, you must manually install the 32-bit libraries.
- For HP-UX Itanium (IA-64) support, you must install the 32-bit HP-UX PA-RISC Oracle or Sybase client. For more information about installing the 32-bit HP-UX PA-RISC Oracle client, see the next topic.

To configure the environment to use a 64-bit database

1. Log in to the computer where you want to install CA Workload Automation AE.
2. Install the 32-bit client for Oracle or Sybase.
3. Do *one* of the following:
   - In the library path (LIBPATH, SHLIB_PATH, or LD_LIBRARY_PATH), ensure that the path to the 32-bit client bin directory precedes the path to the 64-bit client bin directory.
   - If you cannot permanently modify the library path as described in the preceding bullet, modify the path for the local environment.
4. Install the CA Workload Automation AE server.

   The CA Workload Automation AE computer is configured to use the 64-bit version of Oracle or Sybase.

Install the 32-bit HP-UX PA-RISC Oracle Client

To use the 64-bit version of Oracle, you must install the 32-bit client. If you have the following environment:

- CA Workload Automation AE on HP-UX Itanium (IA-64)
- 64-bit version of Oracle

You must install the 32-bit HP-UX PA-RISC Oracle client if it is not already installed. Do this procedure before you install CA Workload Automation AE.

Note: The Oracle 32-bit HP-UX Itanium libraries do not work with CA Workload Automation AE. Ensure that you get the PA-RISC version of the client.

To install the 32-bit HP-UX PA-RISC Oracle client

1. Log in to the computer where you want to install CA Workload Automation AE.
2. Go to the Oracle web site (http://www.oracle.com) and search for Instant Client Downloads for HP-UX PA-RISC (32-bit).
3. Download the 32-bit Oracle Instant Client for HP-UX PA-RISC.
4. Create a directory named lib32.
5. Extract the Instant Client Download packages into the lib32 directory.
6. Run the following command:

   `ln -s libclntsh.sl.x.x libclntsh.sl`

   libclntsh.sl.*x.x*

   Specifies the library file that was extracted to the lib32 directory.

   Example: libclntsh.sl.10.1

   A softlink named libclntsh.sl is created for the libclntsh.sl.*x.x* file.
7. Set the following environment variables to the directory where you created the lib32 directory, as shown in the following example:

   ```
   export ORACLE_HOME=/ora32/lib32
   export TNS_ADMIN=/ora32/lib32
   export SHLIB_PATH=/ora32/lib32:$SHLIB_PATH
   ```

   Note: In the SHLIB_PATH variable, ensure that the path to the lib32 directory precedes the path to the 64-bit client bin directory.
8. Install the CA Workload Automation AE server.
9. Open all the CA Workload Automation AE environment scripts, modify the ORACLE_HOME and TNS_ADMIN variables to point to the directories specified in Step 7, and save the scripts. The environment scripts are as follows:
   - $AUTOUSER/autosys.sh.*hostname*—for Bourne shell users
   - $AUTOUSER/autosys.csh.*hostname*—for C shell users

- $AUTOUSER/autosys.ksh.*hostname*—for Korn shell users
- $AUTOUSER/autosys.bash.*hostname*—for Bash shell users

The 32-bit HP-UX PA-RISC Oracle client is installed, and the CA Workload Automation AE computer is configured to use the 64-bit version of Oracle.

Chapter 5: Installing the Server

This chapter describes how to perform attended installations of CA Workload Automation AE.

Note: The UNIX version of CA Workload Automation AE is packaged as a self-installing PIF (CA Product Interchange Format) product. PIF products are compatible with CA Software Distribution Manager (CA SDM). Therefore, you can deploy CA Workload Automation AE to machines in your enterprise through CA SDM. For more information about setting up CA Workload Automation AE to be delivered through CA SDM, see the Software Distribution Manager documentation.

This section contains the following topics:

Installation Considerations

The following are important considerations for server installation:

- Before you install the server, we recommend that you complete your server installation checklist. You can use the information from your checklist during the installation. We recommend that you also review the installation considerations.
- The default installation locations for the various components are as follows:
  - CA Workload Automation AE— /opt/CA/WorkloadAutomationAE
  - CA common components— /opt/CA/SharedComponents

    Notes:

    - You cannot specify another target installation directory if a CA common component or CA Workload Automation AE r11.3 component is already installed on your computer.
    - You must specify a different installation directory if Unicenter AutoSys JM 4.5 or r11 is already installed on your computer. Otherwise Unicenter AutoSys JM 4.5 or r11 is rendered unusable.
- If you select a component with a dependency on any other component, the associated component is automatically selected for installation.
- You can opt to perform a New or Standalone installation. Choosing Standalone lets you install only the SDK or product documentation.
- You can install CA common components such as CA EEM or Event Management from the CA Common Components DVD, available separately. If you choose to install these common components, we recommend you install them first and then install CA Workload Automation AE. For information about installing common components, see the *CA Common Components Implementation Guide*.
- If you install CA Workload Automation AE and Unicenter NSM Job Management Option 3.1(JMO) on the same computer, some of the Unicenter JMO components may not work as expected. To prevent this, you must follow these steps before you install CA Workload Automation AE:

  1. Issue the following command:

     ```
     echo $TERM
     ```

     The terminal code is obtained.

  2. Issue the following command:

     ```
     env –i bash
     ```

     The environment is cleared.

  3. Export the TERM environment variable to the same value that you obtained in Step 1.

  4. Source the /etc/profile.CA (for CA Workload Automation AE) and /etc/profile.uni (for Unicenter JMO) scripts.

Required Licenses

You need the following licenses:

- A single scheduler license. The corresponding license key is 2WAS.
- An agent license with usage count equal to the number of total machines (excluding virtual machines) defined in CA Workload Automation AE. The corresponding license key is 2WAA.

Notes:

- All licensing checks occur server side (on the scheduler machine).
- You must get the scheduler and agent license keys and place them in the ca.olf file. The ca.olf file is located in the /opt/CA/SharedComponents/ca_lic directory on the scheduler machine. For more information about getting and applying licenses, contact Technical Support at http://ca.com/support.

Agent Installed on the Server Computer

When you install the server, the agent is installed on the server computer. You can use this agent to run jobs on the server computer.

Note: The agent is installed on the server computer whether you perform a typical or custom server installation. If you perform a custom server installation, you can select whether you want to install the application server, client, SDK, or documentation components.

How to Install the Server

The server is the core of the CA Workload Automation AE system and is installed with a scheduler, application server, agent, SDK, and client tools. This topic provides an overview of the steps that you must perform to complete the installation of the server.

Note: For information about system requirements, see the *Release Notes*. We recommend that you review this document before you begin the installation.

To complete the installation of the server, follow these steps:

1. Install the event server database. The supported databases are Sybase and Oracle. For more information, contact your database vendor.
2. Collect the required information (see page 71).

   Note: You can use the Installation Checklist for the CA Workload Automation AE Server to collect the required information before you run the installation.
3. Install the server (see page 85).
4. Define the agent on the server (see page 88).
5. Verify the installation (see page 89).

Installation Checklist for the CA Workload Automation AE Server

This checklist describes the prompts that appear during the interview phase of the CA Workload Automation AE server installation. Default values are provided for fields that require text or numeric input.

You can install the server using either of the following installation types:

- Typical—Requires minimal user input. This mode is suitable for most installations.
- Custom—Requires significant user input. This mode is suitable for advanced users.

The components (see page 50) installed during a typical server installation are as follows:

- Scheduler
- Application Server
- Agent
- Client
- SDK
- Documentation
- Command Sponsor

Note: After you have gathered the information requested in this checklist, see the host machine checklist and complete it.

Information Requested	Installation Type	Your Selection or Value
Installation Definition The definition of the installation to perform: ■ Server ■ Client ■ Agent	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
Installation Type The type of installation to perform: ■ Typical ■ Custom Whether you want the installation to update the login profile files in the /etc directory. **Note:** If you clear the Profile Update check box, you must manually update the profile files after the installation is complete and before CA Workload Automation AE can function. For information about updating the login profile files, see the installation log.	Typical or Custom	
Components The components to install.	Custom	
Installation Path The CA Workload Automation AE installation path. The default installation path is /opt/CA/WorkloadAutomationAE. The CA Common Components installation path. The default installation path is /opt/CA/SharedComponents. **Note:** If other CA Workload Automation AE components or the CA Common Components are already installed, the respective directory field is disabled and the directory where the other CA Workload Automation AE components or the CA Common Components are installed is displayed. We recommend that all CA Workload Automation AE components be installed in the same directory, and all CA Common Components be installed in the same directory.	Custom	
Instance Information The CA Workload Automation AE instance ID, which is an uppercase, three-character alphanumeric name that identifies a specific installation of CA Workload Automation AE. The default instance ID is ACE.	Typical or Custom	
Data Encryption The type of data encryption. You can select either the Default or a Custom Key. If you select Custom Key, you must also specify the key format and key contents. A passphrase format specifies 1-16 alphanumeric characters. A hexadecimal format specifies exactly 32 alphanumeric characters, consisting of 0-9 or A-F. **Note:** If the key entered in Verify Key does not exactly match the key entered in Key, you will get an error.	Custom	

Information Requested	Installation Type	Your Selection or Value
Application Server and Scheduler Information The application server host name. The name of the host computer where the application server is installed is the default. The application server port number. The default port number is 9000. **Limits:** 0-65535 The application server auxiliary port number. The default auxiliary port number is 7500. **Limits:** 0-65535 The scheduler auxiliary listening port. The default port number is 7507. Whether you want to create CA EEM security policies for this instance. You can select Do not use EEM with this instance, Create or re-create EEM security policies for this instance, or Create or use existing EEM security policies for this instance option from the drop-down list. The Create or re-create EEM security policies for this instance option is selected by default. **Note:** CA EEM security policies control asset-level security, depending on the set policy rules. If you select the Create or re-create EEM security policies for this instance or Create or use existing EEM security policies for this instance option, you must have CA EEM installed locally or on a remote host.	Typical	
Application Server Information The application server host name. The name of the host computer where the application server is installed is the default. The application server port number. The default port number is 9000. **Limits:** 0-65535 The application server auxiliary port number. The default auxiliary port number is 7500. **Limits:** 0-65535 Whether you want to create CA EEM security policies for this instance. You can select Do not use EEM with this instance, Create or re-create EEM security policies for this instance, or Create or use existing EEM security policies for this instance option from the drop-down list. The Create or re-create EEM security policies for this instance option is selected by default. **Note:** CA EEM security policies control asset-level security, depending on the set policy rules. If you select the Create or re-create EEM security policies for this instance or Create or use existing EEM security policies for this instance option, you must have CA EEM installed locally or on a remote host.	Custom	

Information Requested	Installation Type	Your Selection or Value
Embedded Entitlements Manager Properties **Note:** This page is displayed only if you selected the Create or re-create EEM security policies for this instance or Create or use existing EEM security policies for this instance option on the Application Server and Scheduler Information (Typical) or Application Server Information (Custom) page. ■ Security Server Name ■ EEM Administrator : EiamAdmin (grayed out) ■ The password of the CA EEM administrator user (EiamAdmin) **Note:** You will be prompted for this password when you install CA Workload Automation AE that uses CA EEM.	Typical or Custom	
Embedded Entitlements Manager Server Test **Note:** This page is displayed only if you selected the Create or re-create EEM security policies for this instance or Create or use existing EEM security policies for this instance option on the Application Server and Scheduler Information (Typical) or Application Server Information (Custom) page. Whether the CA EEM server connection is valid. You must click Test to perform a validation on your server connection to proceed.	Typical or Custom	
Application Server Properties The application server settings: ■ Whether you want the application server to start automatically at system startup time. This check box is selected by default. ■ Whether you want the application server to start immediately after installation. This check box is selected by default. ■ Whether you want to restart the iGateway immediately after installation. This check box is selected by default. ■ Whether you want to configure the CA Workload Automation AE instance for a highly-available clustered environment to protect the CA Workload Automation AE startup options, so that the Cluster support can function properly. This check box is not selected by default.	Custom	
Database Type The database type for the CA Workload Automation AE instance. The available database types are Oracle and Sybase. (Custom only) Whether you want to employ dual event servers in your environment to specify a primary server and a secondary server, in case the primary server fails for some reason.	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
Note: The next several rows in this table describe the Oracle pages. If you have selected Sybase, you can skip to the Sybase rows in this table.		
Oracle Only		
Primary Event Server Properties The event server settings: ■ The Net8/Oracle Net TNS alias (Oracle service name) for the event server that contains the database. CA Workload Automation AE requires that Net8/Oracle Net be installed on the database computer. The TNS alias name must be configured in the Oracle tnsnames.ora configuration file. ■ The Oracle Home location where the existing Oracle database is or where you want to create it. ■ The location of the tnsnames.ora file in the TNS_ADMIN directory. The system TNS configuration file is tnsnames.ora. You must specify the path to the tnsnames.ora file. ■ The storage management option to use. You can select Not using Oracle storage management, Using Oracle Managed Files (OMF), or Using Automatic Storage Management (ASM) from the drop-down list. ■ Whether you want to create the database (if the CA Workload Automation AE database does not exist), refresh the database (if the CA Workload Automation AE database is already installed), or skip creating or refreshing the database. This check box is selected by default. If you clear this check box, the installer does not create the database or the tablespaces. ■ Whether you want to create the tablespaces. This check box is selected by default. If you clear this check box, you must create the database tablespaces manually.	Typical or Custom	
Database Administrator Information The name of the user who is granted the database administrator role for the database. The password of the user who is granted the database administrator role for the database.	Typical or Custom	
Database Connection Test Whether the database connection is valid. You must click Test to perform a validation on your database connection to proceed.	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
Database User Information Administrator User: aedbadmin (grayed out). The password of the database administrator user. Database User: autosys (grayed out). The password of the database user.	Typical or Custom	
Database Tablespace Information If you select to create the database tablespaces in the Primary Event Server Properties page: ■ The name of the tablespace on the event server that contains the database tables, and the database tablespace size in megabytes. The default database tablespace name is AEDB_DATA. The default tablespace size is 800 MB. The minimum size is 400 MB. ■ The name of the tablespace on the event server that contains the database indexes, and the index tablespace size in megabytes. The default index tablespace name is AEDB_INDEX. The default tablespace size is 80 MB. The minimum size is 40 MB. ■ The directory where you want to create the data tablespace and the directory where you want to create the index tablespace. These directories must already be defined on the Oracle server. If you select not to create the database tablespaces in the Primary Event Server Properties page: ■ The name of the tablespace on the event server that has already been created. This tablespace contains the database tables. ■ The name of the tablespace on the event server that has already been created. This tablespace contains the database indexes.	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
Secondary Event Server Properties **Note:** This page is displayed only if you selected the Employ Dual Event Servers check box on the Database Type page. The secondary event server settings: ■ The Net8/Oracle Net TNS alias (Oracle service name) for the event server that contains the database. CA Workload Automation AE requires that Net8/Oracle Net be installed on the database computer. The TNS alias name must be configured in the Oracle tnsnames.ora configuration file. ■ The storage management option to use. You can select Not using Oracle storage management, Using Oracle Managed Files (OMF), or Using Automatic Storage Management (ASM) from the drop-down list. ■ Whether you want to create the database (if the CA Workload Automation AE database does not exist), refresh the database (if the CA Workload Automation AE database is already installed), or skip creating or refreshing the database. This check box is selected by default. If you clear this check box, the installer does not create the database or the tablespaces.	Custom	
Database Administrator Information The name of the user who is granted the database administrator role for the database. The password of the user who is granted the database administrator role for the database.	Custom	
Database Connection Test Whether the database connection is valid. You must click Test to perform a validation on your database connection to proceed.	Custom	

Information Requested	Installation Type	Your Selection or Value
Database Tablespace Information If you select to create the database tablespaces in the Secondary Event Server Properties page: ■ The name of the tablespace on the second event server that contains the database tables, and the database tablespace size in megabytes. The default database tablespace name is AEDB_DATA. The default tablespace size is 800 MB. The minimum size is 400 MB. ■ The name of the tablespace on the second event server that contains the database indexes, and the index tablespace size in megabytes. The default index tablespace name is AEDB_INDEX. The default tablespace size is 80 MB. The minimum size is 40 MB. ■ The directory where you want to create the data tablespace and the directory where you want to create the index tablespace. These directories must already be defined on the Oracle server. If you select not to create the database tablespaces in the Secondary Event Server Properties page: ■ The name of the tablespace on the second event server that has already been created. This tablespace contains the database tables. ■ The name of the tablespace on the second event server that has already been created. This tablespace contains the database indexes.	Custom	

Information Requested	Installation Type	Your Selection or Value
Sybase Only		
Primary Event Server Properties The event server settings: ■ The name of the Sybase server where you want to install the database for the primary event server. ■ The path of the Sybase directory on the server. ■ The name of the database on the Sybase server. The default database name is AEDB. ■ Whether you want to create the database (if the CA Workload Automation AE database does not exist), refresh the database (if the CA Workload Automation AE database is already installed), or skip creating or refreshing the database. This check box is selected by default. If you clear this check box, you must later specify the name of the CA Workload Automation AE database that is already installed. ■ Whether you want to create new database devices. This check box is selected by default. If you clear this check box, you must create the database devices manually.	Typical or Custom	
Database Administrator Information The name of the database user who is granted the database administrator role for the database. The password of the database user who is granted the database administrator role for the database. Database User: autosys (grayed out). The password of the database user.	Typical or Custom	
Database Connection Test Whether the database connection is valid. You must click Test to perform a validation on your database connection to proceed.	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
Data Device Information If you select to create the database device in the Primary Event Server Properties page: ■ The directory where you want to create the Sybase data device. This directory must exist on the Sybase server. ■ The name of the data device. The default data device name is AEDB_DATA. ■ The size (in megabytes) of the data device. The default size is 800 MB. The minimum size is 400 MB. ■ Whether you want to create the log repository on a separate device. This check box is selected by default. If you select not to create the data device in the Primary Event Server Properties page: ■ The name of the already created device. ■ Whether you want the log repository on a separate device. This check box is selected by default. ■ The name of the already created device, if you want the log repository on a separate device.	Typical or Custom	
Log Device Information This page is displayed only if you selected to create the log device in the Data Device Information page: ■ The directory where you want to create the Sybase log device. This directory must exist on the Sybase server. ■ The name of the log device. The default log device name is AEDB_LOG. ■ The size (in megabytes) of the log device. The default size is 100 MB. The minimum size is 50 MB.	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
Secondary Event Server Properties The secondary event server settings: ■ The name of the Sybase server where you want to install the database for the second event server. ■ The name of the database on the Sybase server. The default database name is AEDB. ■ Whether you want to create the database (if the CA Workload Automation AE database does not exist), refresh the database (if the CA Workload Automation AE database is already installed), or skip creating or refreshing the database. This check box is selected by default. If you clear this check box, you must later specify the name of the CA Workload Automation AE database that is already installed. ■ Whether you want to create new database devices. This check box is selected by default. If you clear this check box, you must create the database devices manually.	Custom	
Database Administrator Information The name of the database user who is granted the database administrator role for the database. The password of the database user who is granted the database administrator role for the database.	Custom	
Database Connection Test Whether the database connection is valid. You must click Test to perform a validation on your database connection to proceed.	Custom	

Information Requested	Installation Type	Your Selection or Value
Data Device Information If you select to create the database device in the Secondary Event Server Properties page: ■ The directory where you want to create the Sybase data device. This directory must exist on the Sybase server. ■ The name of the data device. The default data device name is AEDB_DATA. ■ The size (in megabytes) of the data device. The default size is 800 MB. The minimum size is 400 MB. ■ Whether you want to create the log repository on a separate device. This check box is selected by default. If you select not to create the data device in the Secondary Event Server Properties page: ■ The name of the already created device. ■ Whether you want the log repository on a separate device. This check box is selected by default. ■ The name of the already created device, if you want the log repository on a separate device.	Custom	
Log Device Information This page is displayed only if you selected to create the log device in the Data Device Information page: ■ The directory where you want to create the Sybase log device. This directory must exist on the Sybase server. ■ The name of the log device. The default log device name is AEDB_LOG. ■ The size (in megabytes) of the log device. The default size is 100 MB. The minimum size is 50 MB.	Custom	
End of database-specific pages		

Information Requested	Installation Type	Your Selection or Value
Scheduler Properties The scheduler auxiliary port number. The default auxiliary port number is 7507. The scheduler settings: ■ Whether you want the scheduler to automatically start at system start time. This check box is selected by default. ■ Whether you want the scheduler to start immediately after installation. This check box is selected by default. ■ Whether you want to configure high availability. Do not select the Configure High Availability check box if the scheduler will be controlled with a cluster system. ■ The level of cross-platform scheduling. You can set the cross-platform scheduling to Off, Manager only, or Manager and Agent only. The default is Off.	Custom	
High Availability **Note:** This page is displayed only if you selected the Configure High Availability check box on the Scheduler Properties page. The host name of the additional application servers for high availability. The scheduler role for high availability. You can set the scheduler to function as a primary, shadow, or tie-breaker scheduler. The default is Primary. The host name of the primary scheduler. If you select Shadow or Tie-Breaker from the Scheduler Role drop-down list, you must specify the host name of the primary scheduler in this field.	Custom	

Information Requested	Installation Type	Your Selection or Value
Agent Information The agent settings: ■ Whether you want to use an existing agent for the installation. If so, the name and port number of the existing agent. If not, specify the name and port of the agent that will be installed. The default agent name is WA_AGENT. The default port number is 7520. If port multiplexing is selected, the default port number is 49154. ■ Whether you want the agent to automatically start at system start time. This check box is selected by default. ■ Whether you want the agent to start immediately after installation. This check box is selected by default. ■ Whether you want to enable SNMP capabilities. ■ Whether you want to enable port multiplexing. ■ A temporary directory that is required for the agent installation process. It must be an existing directory with at least 260 MB of free space.	Custom	
SNMP Information **Note:** This page is displayed only if you selected the Enable SNMP capabilities check box on the Agent Information page. The SNMP settings: ■ Whether to control the agent using SNMP. This check box is selected by default. ■ The SNMP host name. The name of the host computer where CA Workload Automation AE is installed is the default. ■ The SNMP control port. The default value is 161. ■ Whether to enable support for the SNMP job type. This check box is selected by default. ■ The SNMP trap listener port. The default value is 162.	Custom	

Information Requested	Installation Type	Your Selection or Value
(AIX only) JRE Directory Path The JRE directory. **Note:** You must specify the full directory path of the JRE location. The java directory. **Note:** You must specify the full directory path of the java program.	Typical or Custom	
Owner and Group Settings The name of the owner and group for the CA Workload Automation AE product files. The default owner name is autosys. The default group name is sys. Whether the installation should create the owner or group account if they are not defined on the server. This check box is selected by default.	Custom	

This completes the information requested during the installation of the CA Workload Automation AE server.

More information:

Host Machine Checklist (see page 51)
Install the Server (see page 85)
CA Secure Socket Adapter (SSA) (see page 200)

Install the Server

You can install the server using the installation wizard. The server installation sets up the database and various configuration files, and configures the server computer to run as a client also. This enables you to run jobs on a server computer.

Note: You can install the server using the CA Workload Automation AE media or by downloading the ISO file by logging in to *Download Center, Products* in the CA Support Online website (http://support.ca.com).

To install the server

1. Log in as root.
2. Mount the CA Workload Automation AE media.

3. Change directories to the mounted file system and run the following command:

   ```
   ./wa_setup.sh
   ```

   The Welcome page appears.

4. Click Next.

   The License Agreement page appears.

5. Read the license text. When you have scrolled to the bottom of the license text, the I Agree button is enabled. If you agree with the license agreement, click I Agree.

   Note: If you click I Disagree, you cannot continue with the installation.

   The Installation Function page appears.

6. Select New and click Next.

   The Installation Definition page appears.

7. Select Server and click Next.

   The Installation Type page appears.

8. Continue with the installation by entering the required information in each wizard page and clicking Next.

   After you complete the last data entry page of the wizard and click Next, the Review Settings page appears, listing the information you entered.

9. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the installation completes, the Installation Complete page appears.

   Note: If you want to view the readme, you must click the Readme button on the Installation Complete page. The readme includes information about the known issues in this release.

10. Click Finish.

    The server installation is complete.

More information:

Installation Checklist for the CA Workload Automation AE Server (see page 71)
Installing the Server, Client, or Agent Silently (see page 149)

wa_setup.sh—Install, Update, or Remove CA Workload Automation AE

You can install, update, or remove CA Workload Automation AE using the shell script, wa_setup.sh. It can also be used to generate a response file for a silent installation and to perform a silent installation. When you run wa_setup.sh, you specify the appropriate options depending on what functions you want to perform.

The following options are available:

-a *response_file*

Creates only a response file with the specified name. This response file can be used during a later installation of CA Workload Automation AE.

-F

Forces the CA Workload Automation AE installation, ignoring backup errors. When updating an existing installation, wa_setup.sh first backs up the existing installation in case the update fails. Normally, if the backup fails, then the update cannot occur. However, this option specifies to ignore the backup errors and continue with the CA Workload Automation AE installation.

-h|-?

Displays the usage statement.

-p *log_file*

Logs the installation in the specified file. If this option is not specified, the installation log is stored in /opt/CA/installer/log.

Note: If the installation abnormally terminates, the installation log is stored in /tmp or the directory specified in $TMPDIR.

-r *response_file*

Installs CA Workload Automation AE using the specified response file. You must specify the full path. This option is used in with the -s option.

-s

Installs CA Workload Automation AE in unattended (silent) mode. If the -r option is not used, default parameters are used.

-t *trace_file*

Traces the installation to the specified file. You must specify the full path.

-v

Displays the version of the installer.

-x

Extracts only CA Workload Automation AE to the /tmp directory or the directory specified in $TMPDIR. The file name used for the extracted CA Workload Automation AE is internally-defined and displayed on the command line.

-agent

Installs only the agent. This option lets you bypass the installation wizard pages not directly associated with the typical agent installation.

Note: You can also install the agent using the agent_setup.sh script. The agent installed using either wa_setup.sh or agent_setup.sh is the same.

-client

Installs the client and agent. This option lets you bypass the installation wizard pages not directly associated with the typical client installation.

-server

Installs the scheduler, application server, client, and agent. This option lets you bypass the installation wizard pages not directly associated with the typical server installation.

More Information:

Install the Agent Using agent_setup.sh (see page 113)

Define the Agent on the Server

To enable communication between CA Workload Automation AE and the agent, you must define the agent (see page 117) that is installed with the server to the database.

Note: You must ensure that the parameters you specify when you define an agent on CA Workload Automation AE match the corresponding parameters in the agent's agentparm.txt file.

More Information:

Modify the Encryption Type and Encryption Key on CA Workload Automation AE (see page 168)
agentparm.txt File (see page 163)

How to Verify the Server Installation

Before continuing with the post-installation procedures that may include creating additional EDIT and EXEC superusers and installing clients, you must test the product to make sure it is installed properly.

To verify the server installation, do the following:

1. Set the time zone on the scheduler (see page 89).
2. Set up the server environment (see page 90).
3. Start the scheduler (see page 90).
4. Start the application server (see page 91).
5. Verify that the agent is working and the database is accessible (see page 91).
6. Run a test job (see page 95).
7. Test the environment setup (see page 96).

Set the Time Zone

Before you start the scheduler, make sure that the TZ environment variable is set. The scheduler references this setting to determine the default time zone. Jobs with time-based starting conditions that do not specify a time zone have their start event scheduled based on the time zone under which the scheduler runs. This time zone is also used to report event times, using the autorep command.

Set Up the Environment

To set up the environment, you must log on to the server computer as the owner of CA Workload Automation AE (for example, *autosys*) and source the proper file in AUTOUSER. (Because AUTOUSER is not defined yet, you must enter the full path.)

In the following examples, fiji is the name of the server computer, /opt/CA/WorkloadAutomationAE represents the path to the directory where you installed CA Workload Automation AE, and ACE is the name of the CA Workload Automation AE instance.

If you are running the C shell (csh), enter the following command:

```
source /opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.csh.fiji
```

If you are running the Bourne shell (sh), enter the following command:

```
. /opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.sh.fiji
```

If you are running the Korn shell (ksh), enter the following command:

```
. /opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.ksh.fiji
```

If you are running the Bash shell (bash), enter the following command:

```
. /opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.bash.fiji
```

Start the Scheduler

To start the scheduler, enter the following command:

```
eventor
```

When eventor is run, you lose control of the open command prompt window. To run any other commands while the eventor is running, you must open a new command window. This lets you view the eventor output while running commands through the second command prompt.

To let the eventor run silently and return a command prompt, enter the following command:

```
eventor –q
```

This lets you manually scroll through the eventor output without losing the command prompt.

Note: The eventor script is designed to make sure that the environment is in the right state before starting the scheduler; specifically, it ensures that another scheduler is not already running.

More information:

Set the Time Zone (see page 89)
Startup Scripts (see page 151)

Start the Application Server

To start the application server, enter the following command at the operating system prompt:

```
as_server -A $AUTOSERV
```

More information:

Startup Scripts (see page 151)

Verifying the Agent and Database Accessibility

You can use the autoping command to do the following:

- Verify that the agent on the server computer is functioning.
- Check the computer's database connection. If you are running dual event servers, the autoping command checks both the databases.

More information:

Verify Agent Accessibility (see page 92)
Verify Database Connection (see page 92)

Verify Agent Accessibility

You can verify that an agent is functional and set up properly by running the autoping command to ping the agent from the server or client computer.

Note: After you install the agent, you must define that agent on CA Workload Automation AE (see page 117) to enable communication between CA Workload Automation AE and the agent. So, you must ensure that the agent is defined on CA Workload Automation AE before you verify the agent accessibility.

To verify that the agent is functional on the server computer, enter the following command:

```
autoping -m servername
```

servername

Specifies the name of the server computer.

The following message appears:

```
AutoPinging Machine [servername]
AutoPing WAS SUCCESSFUL!
```

If you do not get this message, the agent is not configured properly and, as a result, CA Workload Automation AE cannot start jobs on that computer (even if it is the same computer as the server).

Note: For more information about troubleshooting, see the *User Guide*.

Verify Database Connection

You can check the running status of the database. If you are running dual event servers, the autoping command checks both the databases.

To check the database connection on the computer, enter the following command:

```
autoping -m servername -S
```

servername

Specifies the name of the server computer.

The following message appears:

```
AutoPinging Machine [servername]
AutoPing WAS SUCCESSFUL!
```

If you do not get this message, the database is not accessible.

Note: For more information about troubleshooting, see the *User Guide*.

Running a Test Job

You can test your configured installation and verify your CA Workload Automation AE environment by running a test job.

If the instance is being controlled by CA EEM, before executing any command line interface, first verify that the CA Workload Automation AE subscriber security word is set by running the CA Workload Automation AE Secure Utility (autosys_secure).

Notes:

- For more information about autosys_secure, see the *Reference Guide*.
- For information about configuring CA Workload Automation AE to work with CA EEM, see the *CA Workload Automation Security Guide*.

Job definitions are specified using Job Information Language (JIL). The jil command is a language processor that parses the language and updates the database.

A test job named test_install is included with the product. Its job definition is in the file named $AUTOSYS/test/jil/test_install. If you view this job definition in a text editor, you see the following:

```
# JIL file to test the installation
#  It will write a line to the Output File
insert_job: test_install
machine: localhost
command: /bin/echo “AUTOSYS install test”
std_out_file: /tmp/test_install.out
std_err_file: /tmp/test_install.err
```

Use the test_install job as a template to verify the installation.

Note: If your computer is not aliased to localhost, you must modify the test_install job definition to specify your computer’s actual name.

More information:

Specify a Computer Name in the test_install Job (see page 94)
Add the Test Job to the Database (see page 94)
Run the Test Job (see page 95)
Verify the Test Job (see page 95)

Specify a Computer Name in the test_install Job

If your computer is not aliased to localhost and you intend to use the test job provided with the product, you must modify the test_install job to specify your computer's actual name.

To specify a computer name

1. Open $AUTOSYS/test/jil/test_install to modify the line that reads as follows:

   ```
   machine: localhost
   ```

2. Replace localhost with your computer's host name. For example, you could use the following:

   ```
   machine: myhost
   ```

   Note: This name must match the value you entered in the insert_machine subcommand when you defined the agent to the database.

3. Save and close the test_install file.

Add the Test Job to the Database

After you have modified the test_install job, you must insert it into the database.

To insert the test_install job into the database, enter the following command:

```
jil < $AUTOSYS/test/jil/test_install
```

The following message appears:

```
Insert/Updating Job: test_install
Database Change WAS Successful!
```

If there is a problem, the following message and some error messages appear:

```
Database change was NOT successful
Exit Code = 1
```

Note: To run the test_install job, an event must be sent to cause the job to start.

Run the Test Job

To send an event to start the test_install job, enter the following command:

```
sj test_install
```

This command starts the test_install job by using the sj alias that is defined in the environment file. The sj alias represents the full command line as follows (which could also be used to start the job, if you do not have the aliases defined):

```
sendevent -E STARTJOB -J test_install
```

The event to start the job is now in the database, but the job itself does not start until the scheduler is up and running.

Verify the Test Job

To verify that the job started and ran successfully, monitor the scheduler output log with the following command:

```
autosyslog -e
```

If the job ran successfully, the following message is written to the /tmp/test_install.out file:

```
AUTOSYS install test
```

This indicates that the basic CA Workload Automation AE environment is set up properly.

If the job did not run successfully, you should see an error message indicating the problem in the /tmp/test_install.err file.

To close the scheduler output log, press Ctrl+C on your keyboard.

Test the Environment Setup

After a test job is completed, you must test the navigation through the data server. A successful test confirms that the environment variables needed for CA Workload Automation AE are set up properly.

To test the data server navigation, enter the following command:

```
autorep -J ALL
```

The following message appears:

```
Job Name  Last Start          Last End            ST Run/Ntry  Pri/Xit
--------- -----------         ------------------- -- ------- ------- ---------
Jobname1  06/24/2009 01:01:01 06/24/2009 01:01:05 SU 3/1
```

If the environment is not set up correctly, diagnostic messages are displayed to inform you of what is incorrect. For example:

```
CAUAJM_E_10029 Communication attempt with the Workload Automation AE Application
Server has failed! [machine1:9,000]
CAUAJM_E_10221 Exhausted list of application servers. Failing request.
CAUAJM_E_50033 Error initializing tx subsystem:  CAUAJM_E_10062 Failed to get
initial configuration from Workload Automation AE Application Server(s)
```

Note: For more information about troubleshooting, see the *User Guide*.

Chapter 6: Installing the Client

This chapter describes how to perform attended installations of the CA Workload Automation AE client.

This section contains the following topics:

Installation Considerations

The following are important considerations for client installation:

- Before you install the client, you must ensure that the server was installed successfully and you completed your client installation checklist. You can use the information from your checklist during the installation.
- If you are using the server computer as a client also, that is, running jobs and utilities on the server computer, you do not need to install the client software on the server. The client software is installed during the server installation.

Agent Installed on the Client Computer

When you install the client, the agent is installed on the client computer. You can use this agent to run jobs on the client computer.

How to Install the Client

A client is any executable that interfaces with the application server. A client can run anywhere in the enterprise provided it can reach the computer where the application server is running. This topic provides an overview of the steps that you must perform to complete the installation of the client.

Note: For information about system requirements, see the *Release Notes*. We recommend that you review this document before you begin the installation.

To complete the installation of the client, follow these steps:

1. Verify that a CA Workload Automation AE application server was installed successfully (see page 89).

   Note: You can skip this step if you have already verified a server installation.

2. Collect the required information (see page 98).

   Note: You can use the Installation Checklist for the CA Workload Automation AE Client to collect the required information before you run the installation.

3. Install the client (see page 102).
4. Define the agent on CA Workload Automation AE (see page 103).
5. Verify the installation (see page 103).

Installation Checklist for the CA Workload Automation AE Client

This checklist describes the prompts that appear during the interview phase of the CA Workload Automation AE client installation. Default values are provided for fields that require text or numeric input.

You can install the client using either of the following installation types:

- Typical—Requires minimal user input. This mode is suitable for most installations.
- Custom—Requires additional user input. This mode is suitable for advanced users.

The components (see page 50) installed during a typical client installation are as follows:

- Agent
- Client
- SDK
- Documentation
- CA Secure Socket Adapter (SSA)

Information Requested	Installation Type	Your Selection or Value
Installation Definition The definition of the installation to perform: ■ Server ■ Client ■ Agent	Typical or Custom	
Installation Type The type of installation to perform: ■ Typical ■ Custom Whether you want the installation to update the login profile files in the /etc directory. **Note:** If you clear the Profile Update check box, you must manually update the profile files after the installation is complete and before CA Workload Automation AE can function. For information about updating the login profile files, see the installation log.	Typical or Custom	
Components The components to install.	Custom	
Installation Path The CA Workload Automation AE client installation path. The default installation path is /opt/CA/WorkloadAutomationAE. The CA Common Components installation path. The default installation path is /opt/CA/SharedComponents. **Note:** If other CA Workload Automation AE components or the CA Common Components are already installed, the respective directory field is disabled and the directory where the other CA Workload Automation AE components or the CA Common Components are installed is displayed. We recommend that all CA Workload Automation AE components be installed in the same directory, and all CA Common Components be installed in the same directory.	Custom	

Information Requested	Installation Type	Your Selection or Value
Instance Information The CA Workload Automation AE instance ID, which is an uppercase, three-character alphanumeric name that identifies a specific installation of CA Workload Automation AE. The default instance ID is ACE.	Typical or Custom	
Data Encryption The type of data encryption. You can select either the Default or a Custom Key. If you select Custom Key, you must also specify the key format and key contents. A passphrase format specifies 1-16 alphanumeric characters. A hexadecimal format specifies exactly 32 alphanumeric characters, consisting of 0-9 or A-F. **Note:** If the key entered in Verify Key does not exactly match the key entered in Key, you will get an error.	Custom	
Application Server Information The application server host name. The name of the host computer where the client is installed is the default. The application server port number. The default port number is 9000. **Limits:** 0-65535	Typical or Custom	
Agent Information The agent settings: ■ Whether you want to use an existing agent for the installation. If so, the name and port number of the existing agent. If not, specify the name and port of the agent that will be installed. The default agent name is WA_AGENT. The default port number is 7520. If port multiplexing is selected, the default port number is 49154. ■ Whether you want the agent to automatically start at system start time. This check box is selected by default. ■ Whether you want the agent to start immediately after installation. This check box is selected by default. ■ Whether you want to enable the SNMP capabilities. ■ Whether you want to enable port multiplexing. ■ A temporary directory that is required for the agent installation process. It must be an existing directory with at least 260 MB of free space.	Custom	

Information Requested	Installation Type	Your Selection or Value
SNMP Information **Note:** This page is displayed only if you selected the Enable SNMP capabilities check box on the Agent Information page. The SNMP settings: ■ Whether to control the agent using SNMP. This check box is selected by default. ■ The SNMP host name. The name of the host computer where CA Workload Automation AE is installed is the default. ■ The SNMP control port. The default value is 161. ■ Whether to enable support for the SNMP job type. This check box is selected by default. ■ The SNMP trap listener port. The default value is 162.	Custom	
(AIX only) JRE Directory Path The JRE directory. **Note:** You must specify the full directory path of the JRE location. The java directory. **Note:** You must specify the full directory path of the java program.	Typical or Custom	
Owner and Group Settings The name of the owner and group for the CA Workload Automation AE product files. The default owner name is autosys. The default group name is sys. Whether the installation should create the owner or group account if they are not defined on the server. This check box is selected by default.	Custom	

This completes the information requested during the installation of the CA Workload Automation AE client.

More information:

Host Machine Checklist (see page 51)
Install the Client (see page 102)

Install the Client

You can install the client using the installation wizard. The client installation must be performed on every computer that you use to run, monitor, or define jobs.

Note: You can install the client using the CA Workload Automation AE media or by downloading the ISO file by logging in to *Download Center, Products* in the CA Support Online website (http://support.ca.com).

To install the client

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following command:

   ```
   ./wa_setup.sh
   ```

   The Welcome page appears.
4. Click Next.

   The License Agreement page appears.
5. Read the license text. When you have scrolled to the bottom of the license text, the I Agree button is enabled. If you agree with the license agreement, click I Agree.

   Note: If you click I Disagree, you cannot continue with the installation.

   The Installation Function page appears.
6. Select New and click Next.

   The Installation Definition page appears.
7. Select Client and click Next.

   The Installation Type page appears.
8. Continue with the installation by entering the required information in each wizard page and clicking Next.

   After you complete the last data entry page of the wizard and click Next, the Review Settings page appears, listing the information you entered.

9. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the installation completes, the Installation Complete page appears.

   Note: If you want to view the readme, you must click the Readme button on the Installation Complete page. The readme includes information about the known issues in this release.

10. Click Finish.

    The client installation is complete.

More information:

Installation Checklist for the CA Workload Automation AE Client (see page 98)
Installing the Server, Client, or Agent Silently (see page 149)

Define the Agent on CA Workload Automation AE

To enable communication between CA Workload Automation AE and the agent, you must define the agent (see page 117) that is installed with the client to the database.

Note: You must ensure that the parameters you specify when you define an agent on CA Workload Automation AE match the corresponding parameters in the agent's agentparm.txt file.

How to Verify the Client Installation

To verify the client installation, do the following:

1. Set up the client environment (see page 104).
2. Verify the client (see page 105).

Set Up the Environment

To set up the environment, you must log on to the client computer as the owner of CA Workload Automation AE (for example, autosys) and source the proper file in AUTOUSER. (Because AUTOUSER is not defined yet, you must enter the full path.)

In the following examples, fiji is the name of the server computer, /opt/CA/WorkloadAutomationAE represents the path to the directory where you installed CA Workload Automation AE, and ACE is the name of the CA Workload Automation AE instance.

If you are running the C shell (csh), enter the following command:

```
source /opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.csh.fiji
```

If you are running the Bourne shell (sh), enter the following command:

```
. /opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.sh.fiji
```

If you are running the Korn shell (ksh), enter the following command:

```
. /opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.ksh.fiji
```

If you are running the Bash shell (bash), enter the following command:

```
. /opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.bash.fiji
```

Verify the Client

To verify that the agent is functional on the client computer, enter the following command:

`autoping -m clientname`

clientname

Specifies the name of the client computer.

The following message appears:

```
AutoPinging Machine [clientname]
AutoPing WAS SUCCESSFUL!
```

If you do not get this message, the agent is not configured properly, and as a result, CA Workload Automation AE cannot start jobs on that computer.

Notes:

- After you install the agent, you must define that agent on CA Workload Automation AE (see page 117) to enable communication between CA Workload Automation AE and the agent. So, you must ensure that the agent is defined on CA Workload Automation AE before you verify that the agent is functional on the client computer.
- For more information about troubleshooting, see the *User Guide*.

Chapter 7: Installing the Agent

This chapter describes how to perform attended installations of the agent on UNIX, Linux, or Windows.

Notes:

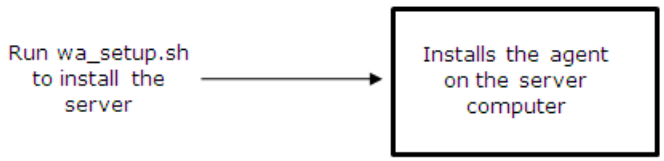
- For more information about installing the agent on i5/OS, see the *CA Workload Automation Agent for i5/OS Implementation Guide*.
- For more information about installing the agent on z/OS, see the *CA Workload Automation Agent for z/OS Installation and Configuration Guide*.

This section contains the following topics:

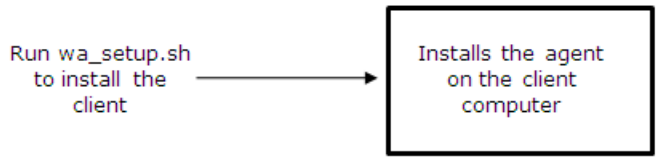
Installation Scenarios

You must install the agent on every computer that you use to run jobs.

When you install the server, the agent is installed by default on the server computer.

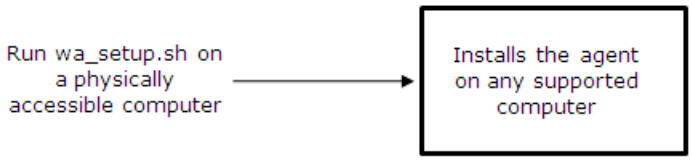


When you install the client, the agent is installed by default on the client computer.

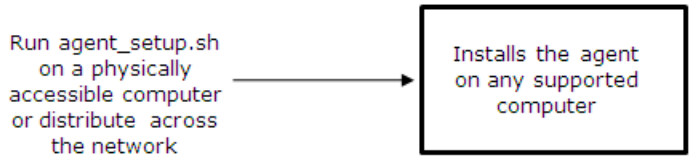


Depending on your requirements, you can install additional agents on other computers using the wa_setup.sh or agent_setup.sh script. We recommend the following guidelines:

- Use the wa_setup.sh script to install the agent on any computer (including the server and client computers) if the computer is physically accessible. The wa_setup.sh script is large in size and may not be as efficient for distributing across your network.



- Use the agent_setup.sh script to install the agent on remote computers or to install multiple agents on a single computer. The agent_setup.sh script is smaller is size than wa_setup.sh and can be distributed across the network.



Note: The agent installed using either wa_setup.sh or agent_setup.sh is the same.

User Account Considerations for UNIX Installations

We recommend that you use the root account to install and start the agent on UNIX. Using the root account lets you run jobs under different user accounts.

If you start the agent with an account other than root, you cannot run jobs under different user accounts because the agent cannot switch users. If you plan to run the agent under a specific user account instead of root, consider the following:

- Verify that the user account has the permissions to access the required directories and run the commands and scripts located on the agent computer.
- You can run the agent under the user account when the agent is installed under root. However, you can only run jobs that belong to the user account. We recommend that you install the agent using the specific user account to avoid permission problems.

How to Install the Agent

The agent is the key integration component of CA Workload Automation AE that lets you automate, monitor, and manage workload on different operating environments, applications, and databases. To run workload on a particular system, you must install an agent on that system. This topic provides an overview of the steps that you must perform to complete the installation of the agent.

Note: For information about system requirements, see the *Release Notes*. We recommend that you review this document before you begin the installation.

To complete the installation of the agent, follow these steps:

1. Check the system requirements.

   Note: For information about system requirements, see the *Release Notes* for the agent.

2. Collect the required information (see page 110).

   Note: Before you install the agent, we recommend that you complete your agent installation checklist. You can use the information from your checklist during the installation.

3. (AIX only) Install JRE (see page 52).
4. Do *one* of the following:
   - Install the agent using agent_setup.sh (see page 113).
   - Install the agent using wa_setup.sh (see page 115).

5. Define the agent on CA Workload Automation AE (see page 117).
6. Verify the installation (see page 120).
7. (Optional) Modify the agent configuration settings (see page 163).

Installation Checklist for the Agent

This checklist describes the prompts that appear during the interview phase of the CA Workload Automation AE agent installation. Default values are provided for fields that require text or numeric input.

You can install the agent using either of the following installation types:

- Typical—Requires minimal user input. This mode is suitable for most installations.
- Custom—Requires additional user input. This mode is suitable for advanced users.

The components (see page 50) installed during a typical agent installation are as follows:

- Agent
- CA Secure Socket Adapter (SSA)

Information Requested	Installation Type	Your Selection or Value
Installation Definition The definition of the installation to perform: ■ Server ■ Client ■ Agent	Typical or Custom	
Installation Type The type of installation to perform: ■ Typical ■ Custom Whether you want the installation to update the login profile files in the /etc directory. **Note:** If you clear the Profile Update check box, you must manually update the profile files after the installation is complete and before CA Workload Automation AE can function. For information about updating the login profile files, see the installation log.	Typical or Custom	
Components The components to install.	Custom	

Information Requested	Installation Type	Your Selection or Value
Installation Path The CA Workload Automation AE agent installation path. The default installation path is /opt/CA/WorkloadAutomationAE. The CA Common Components installation path. The default installation path is /opt/CA/SharedComponents. **Note:** If other CA Workload Automation AE components or the CA Common Components are already installed, the respective directory field is disabled and the directory where the other CA Workload Automation AE components or the CA Common Components are installed is displayed. We recommend that all CA Workload Automation AE components be installed in the same directory, and all CA Common Components be installed in the same directory.	Custom	
Application Server Information The application server port number. The default port number is 9000. **Note:** If the agent must communicate with multiple application servers that are configured to use a port other than the default, you can enter multiple ports by separating each port number with a comma.	Typical or Custom	
Agent Information The agent settings: ■ Whether you want to use an existing agent for the installation. If so, the name and port number of the existing agent. If not, specify the name and port of the agent that will be installed. The default agent name is WA_AGENT. The default port number is 7520. If port multiplexing is selected, the default port number is 49154. ■ Whether you want the agent to automatically start at system start time. This check box is selected by default. ■ Whether you want the agent to start immediately after installation. This check box is selected by default. ■ Whether you want to enable the SNMP capabilities. ■ Whether you want to enable port multiplexing. ■ A temporary directory that is required for the agent installation process. It must be an existing directory with at least 260 MB of free space.	Custom	

Information Requested	Installation Type	Your Selection or Value
SNMP Information **Note:** This page is displayed only if you selected the Enable SNMP capabilities check box on the Agent Information page. The SNMP settings: ■ Whether to control the agent using SNMP. This check box is selected by default. ■ The SNMP host name. The name of the host computer where CA Workload Automation AE is installed is the default. ■ The SNMP control port. The default value is 161. ■ Whether to enable support for the SNMP job type. This check box is selected by default. ■ The SNMP trap listener port. The default value is 162.	Custom	
Data Encryption The type of data encryption. You can select either the Default or a Custom Key. If you select Custom Key, you must also specify the key format and key contents. A passphrase format specifies 1-16 alphanumeric characters. A hexadecimal format specifies exactly 32 alphanumeric characters, consisting of 0-9 or A-F. **Note:** If the key entered in Verify Key does not exactly match the key entered in Key, you will get an error.	Custom	
(AIX only) JRE Directory Path The JRE directory. **Note:** You must specify the full directory path of the JRE location. The java directory. **Note:** You must specify the full directory path of the java program.	Typical or Custom	
Owner and Group Settings The name of the owner and group for the CA Workload Automation AE product files. The default owner name is autosys. The default group name is sys. Whether the installation should create the owner or group account if they are not defined on the server. This check box is selected by default.	Custom	

This completes the information requested during the installation of the CA Workload Automation AE agent.

More information:

Host Machine Checklist (see page 51)
CA Secure Socket Adapter (SSA) (see page 200)

Install the Agent Using agent_setup.sh

You can install the agent using agent_setup.sh. The agent installation must be performed on every computer that you use to run jobs.

Notes:

- The agent installed using either wa_setup.sh or agent_setup.sh is the same.
- agent_setup.sh is smaller is size than wa_setup.sh. So, we recommend that you use agent_setup.sh to install the agent on remote computers or install multiple agents on a single computer.
- If the computer where you want to install the agent is physically accessible, you can use wa_setup.sh because you do not need to transfer the large installation file across the network.

To install the agent using agent_setup.sh

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following commands:

   ```
   cd Agent
   ./agent_setup.sh -I agent_name
   ```

   agent_name

   Defines a unique name for the agent.

   Limits: Up to 16 characters; the first character must be a letter; the name can contain any alphanumeric characters and the special characters @, $, and underscore (_).

   Note: Every agent on the same machine must have a unique name.

   The Welcome page appears.
4. Click Next.

   The License Agreement page appears.
5. Read the license text. When you have scrolled to the bottom of the license text, the I Agree button is enabled. If you agree with the license agreement, click I Agree.

   Note: If you click I Disagree, you cannot continue with the installation.

   The Installation Type page appears.

6. Select Typical and click Next.

   The Review Settings page appears, listing the default settings.

7. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the installation completes, the Installation Complete page appears.

   Note: If you want to view the readme, you must click the Readme button on the Installation Complete page. The readme includes information about the known issues in this release.

8. Click Finish.

   The agent with the specified name is installed.

agent_setup.sh—Install, Update, or Remove the Agent

You can install, update, or remove the agent using the shell script, agent_setup.sh. It can also be used to generate a response file for a silent installation and to perform a silent installation. When you run agent_setup.sh, you specify the appropriate options depending on what functions you want to perform.

Note: The recommended method of installing CA Workload Automation AE agents is with the wa_setup.sh script. Use the agent_setup.sh script to install multiple agents on a single computer or when installing agents across a network.

The following options are available:

-a *response_file*

Creates only a response file with the specified name. This response file can be used for a later installation of the agent.

-F

Forces the agent installation, ignoring backup errors. When updating an existing installation, agent_setup.sh first backs up the existing installation in case the update fails. Normally, if the backup fails, then the update cannot occur. However, this option specifies to ignore the backup errors and continue with the agent installation.

-h|-?

Display the usage statement.

-I *agent_name*

Specifies the name of the agent to install. This option lets you install multiple agents. The default agent name is WA_AGENT.

-p *log_file*

Logs the installation in the specified file. If the -p option is not specified, the installation log is stored in /opt/CA/installer/log.

-r *response_file*

Installs the agent using the specified response file. This option is used in conjunction with the -s option.

-s

Installs the agent in unattended (silent) mode. If the-r option is not used, default parameters are used.

-t *trace_file*

Traces the installation to the specified file.

-T

Specifies a typical agent installation.

-v

Displays the version of the installer.

-x

Extracts only the agent files to the /tmp directory. The file name used for the extracted agent files is internally defined and displayed on the command line.

Install the Agent Using wa_setup.sh

You can install the agent using the installation wizard. The agent installation must be performed on every computer that you use to run jobs.

Notes:

- You can install the agent using the CA Workload Automation AE media or by downloading the ISO file by logging in to *Download Center, Products* in the CA Support Online website (http://support.ca.com).
- If you have installed the CA Workload Automation AE server or client on this computer, the agent is already installed.
- We recommend that you use wa_setup.sh to install the agent only if the computer where you want to install the agent is physically accessible. The wa_setup.sh script is large in size and is not as efficient for distributing across the network.

To install the agent using wa_setup.sh

1. Log in as root.
2. Mount the CA Workload Automation AE media.

3. Change directories to the mounted file system and run the following command:

   ```
   ./wa_setup.sh
   ```

   The Welcome page appears.

4. Click Next.

   The License Agreement page appears.

5. Read the license text. When you have scrolled to the bottom of the license text, the I Agree button is enabled. If you agree with the license agreement, click I Agree.

   Note: If you click I Disagree, you cannot continue with the installation.

   The Installation Function page appears.

6. Select New and click Next.

   The Installation Definition page appears.

7. Select Agent and click Next.

   The Installation Type page appears.

8. Continue with the installation by entering the required information in each wizard page and clicking Next.

   After you complete the last data entry page of the wizard and click Next, the Review Settings page appears, listing the information you entered.

9. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the installation completes, the Installation Complete page appears.

   Note: If you want to view the readme, you must click the Readme button on the Installation Complete page. The readme includes information about the known issues in this release.

10. Click Finish.

    The agent installation is complete.

Define the Agent on CA Workload Automation AE

After you install an agent, you must define that agent on CA Workload Automation AE to enable communication between CA Workload Automation AE and the agent.

Note: When you install additional agents on other computers (other than the client or server), you must define these agents on the computer where the CA Workload Automation AE server or client is installed.

You must ensure that the parameters you specify when you define an agent on CA Workload Automation AE match the corresponding parameters in the agentparm.txt file.

To define an agent on CA Workload Automation AE

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter **jil** at the operating system prompt.

   The JIL command prompt is displayed for the local CA Workload Automation AE instance.
3. Enter the following commands:

```
insert_machine: machine_name
type: a
node_name: address
agent_name: agent_name
port: port_number
encryption_type: NONE | DEFAULT | AES
key_to_agent: key
```

machine_name

Defines a unique name for the agent. When defining jobs, specify this name in the machine attribute.

a

Specifies that the machine is a CA Workload Automation Agent for UNIX, Linux, Windows, i5/OS, or z/OS.

address

(Optional) Defines the IP address or DNS name of the computer where the agent is installed.

Default: The value specified in the insert_machine: *machine_name* command.

Note: If you do not specify the node_name attribute, insert_machine: *machine_name* (the default) must be the DNS name of the agent machine. Otherwise, CA Workload Automation AE cannot connect to the agent.

agent_name

(Optional) Specifies the name of an agent.

Default: WA_AGENT

Notes:

- This name must match the agentname parameter specified in the agentparm.txt file.
- You can specify the alias name for the agent in the agent_name parameter to configure the alias on CA Workload Automation AE. For more information about creating an alias for the agent plug-in, see the appropriate *Implementation Guide* for each agent plug-in.

port_number

(Optional) Specifies the port that the agent uses to listen for traffic.

Default: 7520

Note: This port number must match the communication.inputport parameter in the agentparm.txt file.

NONE | DEFAULT | AES

(Optional) Specifies the type of encryption to be used by the agent. You can set the encryption type to *one* of the following:

NONE

Specifies that the agent uses no encryption.

DEFAULT

Specifies that the agent uses the default encryption key and type. This is the default.

AES

Specifies that the agent uses AES 128-bit encryption.

Note: You must specify a key using the key_to_agent attribute.

key

(Optional) Specifies the key used to encrypt data from CA Workload Automation AE to the agent. This value must match the security.cryptkey parameter in the agent's agentparm.txt file, without the prefix 0x. If the values do not match, CA Workload Automation AE cannot communicate with the agent. You must specify *one* of the following:

- A 32-digit hexadecimal key
- A passphrase with up to 16 characters

4. (Optional) Specify optional machine attributes:
   - character_code
   - description
   - opsys
   - max_load
   - factor
   - heartbeat_attempts
   - heartbeat_freq
5. Enter exit.

   The data is loaded into the database. The agent is defined on CA Workload Automation AE.

Notes:

- For more information about the insert_machine subcommand and the related machine attributes, see the *Reference Guide*.
- For more information about the parameters in the agentparm.txt file, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.*

Example: Define an Agent Using the Default Values

This example defines an agent using the default values for the following attributes: type: a, node_name: sysagt, port: 7520, and agent_name: WA_AGENT.

```
insert_machine: sysagt
```

Example: Define an Agent

This example defines a machine named eagle where the agent WA_AGENT runs on the node myagenthostname and uses 49154 as its main input port.

```
insert_machine: eagle
type: a
agent_name: WA_AGENT
node_name: myagenthostname
port: 49154
max_load: 100
factor: 1.0
```

More Information:

agentparm.txt File (see page 163)
Define the Agent on the Server (see page 88)
Define the Agent on CA Workload Automation AE (see page 103)

How to Verify the Agent Installation

You can verify the agent was installed successfully and that the agent can communicate with CA Workload Automation AE by defining, running, and monitoring a test job.

To verify the agent installation, follow these steps:

1. Set up the agent environment (see page 120).
2. Test communication between CA Workload Automation AE and the agent (see page 121).
3. Define a test job (see page 121).
4. Run the test job (see page 122).
5. Monitor the test job (see page 123).

Set Up the Environment

Before verifying the agent installation, you must set up your environment as follows:

- If you are running the C shell (csh), enter the following command:

  ```
  source /opt/CA/WorkloadAutomationAE/autosys.csh
  ```

- If you are running the Bourne shell (sh), enter the following command:

  ```
  . /opt/CA/WorkloadAutomationAE/autosys.sh
  ```

- If you are running the Korn shell (ksh), enter the following command:

  ```
  . /opt/CA/WorkloadAutomationAE/autosys.ksh
  ```

- If you are running the Bash shell (bash), enter the following command:

  ```
  . /opt/CA/WorkloadAutomationAE/autosys.bash
  ```

Test Communication Between CA Workload Automation AE and the Agent

You can verify that CA Workload Automation AE communicates with the agent by issuing the autoping command to ping the server computer.

To test communication between CA Workload Automation AE and the agent

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   `autoping -m machine_name`

   machine_name

   Specifies the name of the machine where the agent runs.

   The following messages appear, which indicates that autoping was successful:

   ```
   CAUAJM_I_50023 AutoPinging Machine [machine_name]
   CAUAJM_I_50025 AutoPing WAS SUCCESSFUL!
   ```

Notes:

- If you do not get this message, the agent is not configured properly and, as a result, CA Workload Automation AE cannot start jobs on that computer (even if it is the same computer as the server).
- The agent on z/OS does not support connectivity to the application server through the SDK. Therefore, if you issue the autoping command with the -S option for the agent on z/OS, the command skips the connectivity test with the application server.

Define a Test Job

You can define a job, such as a Command job that runs a UNIX script, to test communication between CA Workload Automation AE and the agent.

To define a test job

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter **jil** at the operating system prompt.

   The JIL command prompt is displayed for the local CA Workload Automation AE instance.

3. Enter the following commands:

   ```
   insert_job: job_name
   machine: machine_name
   command: "/usr/bin/sleep" 1
   owner: user@host
   ```

   A test job is defined. The following message appears:

   ```
   CAUAJM_I_50323 Inserting/Updating job: job_name
   CAUAJM_I_50205 Database Change WAS Successful!
   ```

4. Enter exit.

   The data is loaded into the database.

Example: Define an i5/OS Job

This example runs the command named CALC on the i5agent computer.

```
insert_job: i5job_runcmd
job_type: I5
machine: i5agent
i5_name: CALC
```

Run the Test Job

You can verify whether jobs will run on the agent using the test job.

To run the test job

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   sendevent -e STARTJOB -J job_name
   ```

   The sendevent command sends an event to start the test job. The event to start the job is now in the database, but the job itself does not start until the scheduler is up and running.

Monitor the Test Job

You can use the scheduler log to monitor the test job and verify that it started and ran successfully.

To monitor the test job

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   autosyslog -e
   ```

   The scheduler log displays the following messages, which indicates that communication between CA Workload Automation AE and the agent is successful:

   ```
   CAUAJM_I_40245 EVENT: CHANGE_STATUS    STATUS: STARTING        JOB: job_name
   MACHINE: machine_name
   CAUAJM_I_40245 EVENT: CHANGE_STATUS    STATUS: RUNNING         JOB: job_name
   MACHINE: machine_name
   CAUAJM_I_40245 EVENT: CHANGE_STATUS    STATUS: SUCCESS         JOB: job_name
   MACHINE: machine_name
   ```

Notes:

- For more information about the autosyslog command, see the *Reference Guide*.
- For more information about troubleshooting the agent, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.*

Install Multiple Agents on a Single Computer

You can install multiple agents on a single computer. This configuration lets you do the following:

- Distribute the load of the jobs across multiple agents. For example, you can run different jobs for different business applications on the same computer. To do this, you can install an agent for one business application and an agent for the other business application and provide access at the agent level.
- Test maintenance applied to an agent before applying maintenance to the production agent.

Important! If a machine with multiple agents is not available, all workload scheduled on that machine is impacted. To avoid a single point of failure, we recommend that you install agents across multiple machines.

You can install the agents using the installation wizard.

To install multiple agents on a single computer

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following commands:

   ```
   cd Agent
   ./agent_setup.sh -I agent_name
   ```

   agent_name

   Defines a unique name for the agent.

   Limits: Up to 16 characters; the first character must be a letter; the name can contain any alphanumeric characters and the special characters @, $, and underscore (_).

   Note: Every agent on the same machine must have a unique name.

   The Welcome page appears.
4. Click Next.

   The License Agreement page appears.
5. Read the license text. When you have scrolled to the bottom of the license text, the I Agree button is enabled. If you agree with the license agreement, click I Agree.

   Note: If you click I Disagree, you cannot continue with the installation.

   The Installation Type page appears.
6. Select Typical and click Next.

   The Review Settings page appears, listing the default settings.
7. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the installation completes, the Installation Complete page appears.
8. Click Finish.

   The agent with the specified name is installed.
9. Repeat Steps 3-8 for each agent you want to install on the same computer.

Update the Installation or Reinstall an Agent

If necessary, you can update the installation or reinstall the CA Workload Automation AE agent using the installation wizard.

To update the installation or reinstall an existing agent

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following commands to start the installation process:

   ```
   cd Agent
   ./agent_setup.sh
   ```

   The Welcome page appears.
4. Select Update/Reinstall and click Next.

   The Active Components page appears if a CA Workload Automation AE component or a dependant CA Common Service is active.
5. Click Next to shut down the active processes.

   Note: Before you can update the installation or reinstall a component, all dependent CA products must be shut down.

   The Review Settings page appears, listing the default settings.
6. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the update completes, the Update Complete page appears.
7. Click Finish.

   The agent reinstallation is complete.

Remove the Agent

After the agent is installed, you can remove it using the installation wizard.

To remove the agent

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following commands:

   ```
   cd Agent
   ./agent_setup.sh
   ```

4. Select Remove and click Next.

   The Remove Product page appears.

5. Select the Backup the CA Workload Automation AE Agent and restore the old version if the removal fails check box and click Next.

   The Review Removal Settings page appears, listing the default settings.

6. Review the information and, if it is correct, click Remove.

   The Deinstallation Complete page appears.

7. Click Ok.

   The agent is removed.

Chapter 8: Setting Up the Database Manually

This section contains the following topics:

How to Create a CA Workload Automation AE Database

The CA Workload Automation AE server requires a database. By default, the CA Workload Automation AE installer creates the tablespaces (for Oracle) or database devices (for Sybase) and schema objects. However, by using the CA Workload Automation AE silent installer, you can bypass the database setup during the CA Workload Automation AE server installation and then create a database manually. You run the CreateAEDB.pl Perl script to create the tablespaces or database devices and schema objects that form the Event server for CA Workload Automation AE. You can run the script in interactive or console mode.

To create a CA Workload Automation AE database, follow these steps:

1. Run the following script to create a response file for installing the CA Workload Automation AE server:

   `./wa_setup.sh –a response_file`

   When the server is installed, the CreateAEDB.pl script is also installed. During the installation interview, do the following:

   a. Select Server as the install definition and Custom as the type.

   b. On the Application Server Properties panel, clear the following checkboxes:

      - Start the application server following installation
      - Restart the iGateway following installation

c. On the Primary Event Server panel, clear the following checkboxes:

- Create the tablespaces (for Oracle)
- Create new database devices (for Sybase)
- Create or refresh database

d. On the Scheduler Properties panel, clear the Start the scheduler following installation checkbox.

e. On the Agent Properties panel, clear the Start the agent following installation checkbox.

f. Review the settings and click OK.

The response file is created

2. Install the CA Workload Automation AE server in unattended mode using the following command:

```
./wa_setup.sh –s -r response_file
```

Note: The server must be run in unattended mode to bypass the database checks that are performed during an attended install.

3. (For Oracle only) Create an oracle instance using dbca.
4. (For Oracle only) If you will be running CreateAEDB.pl in console mode, create directories for the Oracle data and index tablespace, if they do not exist.
5. Create a directory to store the database creation log.

Note: This directory must be empty before running the CreateAEDB script.

6. Verify that the Oracle or Sybase environment is set properly to run sqlplus (for Oracle) or isql (for Sybase). Then, change to the following directory:

- For Oracle: $AUTOSYS/dbobj/ORA
- For Sybase: $AUTOSYS/dbobj/SYB

7. Run the CreateAEDB script using one of these methods:

- Run the CreateAEDB script in console mode (see page 129).
- Run the CreateAEDB script in interactive mode: for Oracle or for Sybase (see page 135).

The database is created for CA Workload Automation AE.

CreateAEDB Script—Create a Database

The CreateAEDB script creates the database required by CA Workload Automation AE. The script creates the tablespaces (for Oracle) and devices(for Sybase) and all the schema objects.

A CreateAEDB script is included for each database vendor in the following directories:

- $AUTOSYS/dbobj/ORA/CreateAEDB.pl (for Oracle)
- $AUTOSYS/dbobj/SYB/CreateAEDB.pl (for Sybase)

Note: You can enter the CreateAEDB script with no options. You are prompted for the required information line by line.

You can also run the CreateAEDB script in console mode. In this case, the script has the following format:

For Oracle

```
perl ./CreateAEDB.pl "ADB_SID" "ADB_SA_USER" "ADB_SA_PSWD" "ADB_ADMIN_PSWD"
"ADB_WA_DB_PSWD" "JAVA_HOME" "ADB_OUTDIR" "CREATE_TBLSPC" "ADB_TS_DATANM"
"ADB_TS_DATADIR" "ADB_TS_DATASZ" "ADB_TS_IXNM" "ADB_TS_IXDIR" "ADB_TS_IXSZ"
"ADB_DEBUG"
```

For Sybase

```
perl ./CreateAEDB.pl "ADB_DATASERVER" "ADB_DATABASE" "ADB_SA_USER" "ADB_SA_PSWD"
"ADB_WA_DB_PSWD" "JAVA_HOME" "ADB_OUTDIR" "CREATE_DB" "ADB_DV_DATADEV"
"ADB_DV_DATADIR" "ADB_DV_DATASZ" "ADB_DV_LOGDEV" "ADB_DV_LOGDIR" "ADB_DV_LOGSZ"
"ADB_DEBUG"
```

ADB_ADMIN_PSWD

Specifies the Oracle ‘aedbadmin’ user password. If the aedbadmin user is already defined in Oracle, you must specify the valid password. If the aedbadmin user is not defined in Oracle, the Installer creates the user with the specified password.

ADB_DATABASE

Specifies the Sybase database name.

ADB_DATASERVER

Specifies the Sybase server name, as defined in the $SYBASE/interfaces file.

ADB_DEBUG

Indicates whether to set debugging on during the installation, as follows:

- Y—Sets debugging on
- N—Disables debugging

ADB_DV_DATADEV

Specifies the Sybase data device name.

ADB_DV_DATADIR

Specifies the Sybase data device path.

ADB_DV_DATASZ

Specifies the Sybase data device size (in MB). The minimum value 400.

ADB_DV_LOGDEV

Specifies the Sybase log device name.

ADB_DV_LOGDIR

Specifies the Sybase log device path.

ADB_DV_LOGSZ

Specifies the Sybase log device size (in MB). The minimum value is 80.

ADB_OUTDIR

Specifies the directory where you want to store the output from the CreateAEDB script. This directory must already exist and be empty prior to running the CreateAEDB script.

ADB_SA_PSWD

Specifies the Oracle or Sybase system administrator user password.

ADB_SA_USER

Specifies the Oracle or Sybase system administrator user ID.

ADB_SID

Specifies the Oracle SID name.

ADB_TS_DATADIR

Specifies the Oracle data tablespace directory path. This directory must already exist on the Oracle server.

ADB_TS_DATANM

Specifies the Oracle data tablespace name.

ADB_TS_DATASZ

Specifies the Oracle data tablespace size (in MB). The minimum value is 800.

ADB_TS_IXDIR

Specifies the Oracle index tablespace directory path. This directory must already exist on the Oracle server.

ADB_TS_IXNM

Specifies the Oracle index tablespace name.

ADB_TS_IXSZ

Specifies the Oracle index tablespace size (in MB). The minimum value is 80.

ADB_WA_DB_PSWD

Specifies the Oracle or Sybase 'autosys' user password. If the autosys user is already defined in Oracle or Sybase, you must specify the valid password. If the autosys user is not defined in Oracle or Sybase, the installer creates the user with the specified password.

CREATE_DB

Indicates whether to create a database for Sybase, as follows:

- Y—Creates a database
- N—Overwrites the existing database

CREATE_TBLSPC

Indicates whether to create tablespaces for Oracle, as follows:

- Y—Creates the data and index tablespaces
- N—Overwrites the existing tablespaces

JAVA_HOME

Specifies the JAVA_HOME path.

Example: Create Oracle Tablespaces

This example creates Oracle tablespaces in the Oracle orcl instance. The output of the script is stored in the /tmp/adblog directory. The script creates two Oracle tablespaces; one named AEDB_DATA that stores up to 800 MB of data, and another named AEDB_INDEX that stores up to 80 MB of data. The script runs without debugging.

```
perl ./CreateAEDB.pl "orcl" "SYS" "syspassword" "adbpassword" "aspassword"
"/usr/java6/jre" "/tmp/adblog" "Y" "AEDB_DATA" "/home/oracle/oradata" "800"
"AEDB_INDEX" "/home/oracle/oradata" "80" "N"
```

Example: Create a Database on Sybase

This example creates a Sybase database named AEDB on Sybase server LAM04. The script creates two Sybase devices; one for the data and one for the log. The data device is named AEDB_DATA and stores up to 800 MB of data. The log device is named AEDB_LOG and stores up to 80 MB of data.

```
perl ./CreateAEDB.pl "LAM04" "AEDB" "sa" "sapassword" "autosyspw"
"/usr/java6/jre" "/tmp/adblog" "Y" "AEDB_DATA" "/opt/sybase/data" "800"
"AEDB_LOG" "/opt/sybase/data" "80" "N"
```

Run the CreateAEDB Script for Oracle in Interactive Mode

To create the CA Workload Automation AE Oracle tablespaces or load existing tablespaces, you can run the CreateAEDB script in interactive mode. The script prompts you for the required information.

To run the CreateAEDB script for Oracle in interactive mode

1. Issue the following commands:

   ```
   cd $AUTOSYS/dbobj/ORA
   perl ./CreateAEDB.pl
   ```

2. Enter the required information for each of the following prompts:

   Service Identifier?

   Enter the Oracle SID name.

   Default: AEDB

   User name with system admin privileges?

   Enter the Oracle system administrator user ID.

   Default: sys

   SYS user's password?

   Enter the Oracle system administrator user password.

   Default: sys

   Note: When you press Enter to accept the password, CreateAEDB verifies that it can connect to Oracle. If it cannot connect to Oracle, CreateAEDB displays the following message and exits:

   ```
   The userid and password combination for the administrator is incorrect.
   ```

aedbadmin user's password?

Enter the Oracle ‘aedbadmin’ user password.

Default: aedbadmin

Note: If the aedbadmin user is defined in Oracle, you must specify the valid password. If the aedbadmin user is not defined in Oracle, the installer creates the user with the specified password.

autosys user's password?

Enter the Oracle ‘autosys’ user password.

Default: autosys

Note: If the autosys user is defined in Oracle, you must specify the valid password. If the autosys user is not defined in Oracle, the installer creates the user with the specified password.

JRE Directory?

Enter the JAVA_HOME path.

Default: /opt/CA/SharedComponents/JRE/1.5.0_11

3. Enter Y or N when prompted to create the Oracle tablespaces, as follows:

Do you want to create the Oracle Data Tablespace? (Y|N)

If you have previously defined a data tablespace, enter N. Otherwise, enter Y

Default: N

- If you enter N, continue with Step 4
- If you enter Y, you are prompted for the following information:

Data Tablespace name?

Specify the name to create the data tablespace with.

Default: AEDB_DATA

Data Tablespace device path ?

Specify the full path to create the data tablespace device in.

Data Tablespace size MB? ?

Specify the data tablespace size, in MB.

Default: 800

Index Tablespace name?

Specify the name to create the index tablespace with.

Default: AEDB_INDEX

Index Tablespace device path?

Specify the full path to create the index tablespace device in.

Index Tablespace size MB?

Specify the index tablespace size, in MB.

Default: 80

Proceed to Step 5.

4. Enter the data and index tablespace information, as follows:

Data Tablespace name?

Enter the name of the defined data tablespace.

Default: AEDB_DATA

Index Tablespace name?

Enter the name of the defined index tablespace.

Default: AEDB_INDEX

An information summary appears.

5. Enter Y or N when prompted to run the script, as follows:

Are you sure? (Y|N)

Enter Y to execute the script.

Default: N

The CA Workload Automation AE tablespaces are created in Oracle if you chose to create the Oracle tablespaces. Otherwise, the tablespaces are refreshed.

Run the CreateAEDB Script for Sybase in Interactive Mode

To create a CA Workload Automation AE Sybase database and devices, you can run the CreateAEDB script in interactive mode. The script prompts you for the required information.

To run the CreateAEDB script for Sybase in interactive mode

1. Make sure $SYBASE is set, and then issue the following commands:

   ```
   cd $AUTOSYS/dbobj/SYB
   perl ./CreateAEDB.pl
   ```

2. Verify the required information for each of the following prompts:

   Server name?

   Enter the Sybase server name.

   Default: DEFAULT_SERVER

   Database name?

   Enter the name you want the Sybase database to be called.

   Default: AEDB

   User name with system admin privileges?

   Enter the Sybase system administrator user ID.

   Default: sa

   sa user's password?

   Enter the Sybase system administrator user password.

   Default: sa

   Note: When you press Enter to accept the password, CreateAEDB verifies that it can connect to Sybase. If it cannot connect, CreateAEDB displays the following message and exits:

   ```
   The host, userid, and password combination for the administrator is
   incorrect.
   ```

   autosys user's password?

   Enter the Sybase ‘autosys’ user password.

   Default: autosys

   Note: If the autosys user is defined in Sybase, you must specify the valid password. If the autosys user is not defined in Sybase, the installer creates the user with the specified password.

   JRE Directory?

   Enter the JAVA_HOME path.

   Default: /opt/CA/Shared/JRE/1.5.0_11

3. Enter Y or N when prompted to create the Sybase database, as follows:

   Do you want to create a new DB? (Y|N)

   If you have previously defined a Sybase database for CA Workload Automation AE, enter N. Otherwise, enter Y.

   Default: N

   - If you enter N, the script refreshes the database when it runs. Continue with Step 4.
   - If you enter Y, you are prompted for the following information:

   Target data device name?

   Enter the Sybase data device name to be created.

   Default: AEDB_DATA

   Target data device path [/opt/sybase/data/]?

   Enter the Sybase data device path, where the device will be created.

   Default: /opt/sybase/data/

   Target data device size MB?

   Enter the Sybase data device size in MB.

   Default: 800

   Next, you are prompted for the following information related to creating a log device:

   Do you want to create a Log Device? (Y|[N])

   If you have previously defined a Sybase device to be used for logs by CA Workload Automation AE, enter N. Otherwise, enter Y.

   - If you enter N, continue with Step 4.
   - If you enter Y, you are prompted for the following information:

   Target log device name?

   Enter the Sybase log device name to be created.

   Default: AEDB_LOG

   Target log device path?

   Enter the Sybase log device path, where the device will be created.

   Default: /opt/sybase/data/

   Target log device size MB?

   Enter the Sybase log device size in MB.

   Default: 100

   An information summary appears.

4. Enter Y or N when prompted to run the script, as follows:

   Are you sure? (Y|N)

   Enter Y to execute the script.

   Default: N

   The CA Workload Automation AE database is created in Sybase if you chose to create the database. Otherwise, the database is refreshed.

Refreshing a CA Workload Automation AE Database

The RefreshAEDB.pl Perl script is used to refresh, update, or add read-only data in the CA Workload Automation AE database, for example, metadata, real-time resources, and stored procedures. RefreshAEDB should only be run when directed by technical support. You can run the script in interactive or console mode.

Note: The CA Workload Automation AE database must have already been installed before you can use the RefreshAEDB script.

RefreshAEDB Script—Refresh a Database

The RefreshAEDB script updates the database used by CA Workload Automation AE. The script updates the tablespaces (for Oracle) and all the schema objects.

A RefreshAEDB script is included for each database vendor in the following directories:

- $AUTOSYS/dbobj/ORA/RefreshAEDB.pl (for Oracle)
- $AUTOSYS/dbobj/SYB/RefreshAEDB.pl (for Sybase)

Note: You can enter the RefreshAEDB script with no options. You are prompted for the required information line by line.

You can also run the RefreshAEDB script in console mode. In this case, the script has the following format:

For Oracle

```
perl ./RefreshAEDB.pl "ADB_SID" "AEDB_ADMIN_PSWD" "JAVA_HOME" "ADB_OUTDIR"
"ADB_DEBUG_VERIFY"
```

For Sybase

```
perl ./RefreshAEDB.pl "ADB_DATASERVER" "ADB_DATABASE" "ADB_SA_USER" "ADB_SA_PSWD"
"JAVA_HOME" "ADB_OUTDIR" "ADB_DEBUG_VERIFY"
```

ADB_DATABASE

Specifies the Microsoft SQL Server or Sybase database name.

ADB_DATASERVER

Specifies the Microsoft SQL Server or Sybase server name.

ADB_DEBUG_VERIFY

Indicates whether to set debugging on during the update, as follows:

- Y—Sets debugging on
- N—Verifies only the connection parameters (no refresh occurs)

ADB_OUTDIR

Specifies the directory where you want to store the output from the CreateAEDB script. This directory must already exist and be empty prior to running the CreateAEDB script.

ADB_SA_PSWD

Specifies the Microsoft SQL Server, Oracle or Sybase system administrator user password.

ADB_SA_USER

Specifies the Microsoft SQL Server, Oracle or Sybase system administrator user ID.

ADB_SID

Specifies the Oracle SID name.

AEDB_ADMIN_PSWD

Specifies the Oracle ‘autosys’ user password.

JAVA_HOME

Specifies the JAVA_HOME path.

Example: Refresh Oracle Tablespaces

This example updates Oracle tablespaces in the Oracle orcl instance. The output of the script is stored in the /tmp/adblog directory. The script runs without debugging.

```
perl ./RefreshAEDB.pl "orcl" "aspassword" "/usr/java6/jre" “/tmp/adblog” "N"
```

Example: Refresh a Database on Sybase

This example updates a Sybase database named AEDB on Sybase server LAM04. The script runs without debugging.

```
perl ./RefreshAEDB.pl "LAM04" "AEDB" "sa" "sapassword" "/usr/java6/jre"
"/tmp/adblog" "N"
```

Run the RefreshAEDB Script for Oracle in Interactive Mode

To update the CA Workload Automation AE Oracle tablespaces, you can run the RefreshAEDB script in interactive mode. The script prompts you for the required information.

To run the RefreshAEDB script for Oracle in interactive mode

1. Issue the following commands:

   ```
   cd $AUTOSYS/dbobj/ORA
   perl ./RefreshAEDB.pl
   ```

2. Enter the required information for each of the following prompts:

   Service Identifier?

   Enter the Oracle SID name.

   Default: AEDB

   aedbadmin user's password?

   Enter the valid Oracle ‘aedbadmin’ user password.

   Default: aedbadmin

   JRE Directory?

   Enter the JAVA_HOME path.

   Default: /opt/CA/SharedComponents/JRE/1.5.0_11

3. Enter Y or N when prompted to run the script, as follows:

   Are you sure? (Y|N)

   Enter Y to execute the script.

   Default: N

   The CA Workload Automation AE tablespaces are updated.

Run the RefreshAEDB Script for Sybase in Interactive Mode

To update a CA Workload Automation AE Sybase database, you can run the RefreshAEDB script in interactive mode. The script prompts you for the required information.

To run the RefreshAEDB script for Sybase in interactive mode

1. Make sure $SYBASE is set, and then issue the following commands:

   ```
   cd $AUTOSYS/dbobj/SYB
   perl ./RefreshAEDB.pl
   ```

2. Verify the required information for each of the following prompts:

   Server name?

   Enter the Sybase server name.

   Default: DEFAULT_SERVER

   Database name?

   Enter the Sybase database to be called.

   Default: AEDB

   User name with system admin privileges?

   Enter the Sybase system administrator user ID.

   Default: sa

   sa user's password?

   Enter the Sybase system administrator user password.

   Default: sa

   Note: When you press Enter to accept the password, RefreshAEDB verifies that it can connect to Sybase. If it cannot connect, RefreshAEDB displays the following message and exits:

   ```
   The host, userid, and password combination for the administrator is
   incorrect. Exiting...
   ```

   autosys user's password?

   Enter the Sybase ‘autosys’ user password.

   Default: autosys

   Note: If the autosys user is defined in Sybase, you must specify the valid password. If the autosys user is not defined in Sybase, the installer creates the user with the specified password.

   JRE Directory?

   Enter the JAVA_HOME path.

   Default: /opt/CA/Shared/JRE/1.5.0_11

3. Enter Y or N when prompted to run the script, as follows:

   Are you sure? (Y|N)

   Enter Y to execute the script.

   Default: N

   The CA Workload Automation AE database is updated in Sybase.

Chapter 9: Installing the SDK Runtime Environment

This section contains the following topics:

How to Install the SDK Runtime Environment

The SDK runtime environment lets you integrate CA Workload Automation AE programmatically with other CA products and third-party products. You must install the SDK runtime environment on the computer where the other CA product (for example, CA Workload Control Center) is installed. The other CA product uses the SDK to interact with CA Workload Automation AE.

To install the SDK runtime environment, follow these steps:

1. Complete the installation checklist for the SDK runtime environment (see page 144).
2. Install the SDK runtime environment (see page 145).

Installation Checklist for the SDK Runtime Environment

This checklist describes the prompts that appear during the interview phase of the CA Workload Automation AE SDK runtime environment installation. Default values are provided for fields that require text or numeric input.

The components installed during a typical installation are as follows:

- SDK runtime environment
- CA Secure Socket Adapter (SSA)

Information Requested	Your Selection or Value
Installation Path The CA Workload Automation AE SDK runtime environment installation path. The default installation path is /opt/CA/WorkloadAutomationAE. The CA Common Components installation path. The default installation path is /opt/CA/SharedComponents. **Note:** If other CA Workload Automation AE components or the CA Common Components are already installed, the respective directory field is disabled and the directory where the other CA Workload Automation AE components or the CA Common Components are installed is displayed. All CA Workload Automation AE components must be installed together in one directory. All CA Common Components must be installed together in one directory.	
Owner and Group Settings The name of the owner and group for the CA Workload Automation AE product files. The default owner name is autosys. The default group name is sys. Whether the installation should create the owner or group account if they are not defined on the server. This check box is selected by default.	

This completes the information requested during the installation of the CA Workload Automation AE SDK runtime environment.

Install the SDK Runtime Environment Using sdk_setup.sh

The SDK runtime environment provides the libraries required by other CA products that communicate with CA Workload Automation AE. You must install the SDK runtime environment on the computer where the other CA product, such as CA Workload Control Center (WCC), is installed.

To install the SDK runtime environment using sdk_setup.sh

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following commands:

   ```
   cd SDK
   ./sdk_setup.sh
   ```

   The Welcome page appears.
4. Click Next.

   The License Agreement page appears.
5. Read the license text. When you have scrolled to the bottom of the license text, the I Agree button is enabled. If you agree with the license agreement, click I Agree.

   Note: If you click I Disagree, you cannot continue with the installation.

   The Installation Path page appears.
6. Enter the path to the installation directory of the CA product that must communicate with CA Workload Automation AE, and click Next.
7. Continue with the installation by entering the required information in each wizard page and clicking Next.

   The Review Settings page appears, listing the default settings.
8. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the installation completes, the Installation Complete page appears.
9. Click Finish.

   The SDK runtime environment is installed.

Install the SDK Runtime Environment Using sdk_setup.sh

You can install, update, or remove the SDK runtime environment using the shell script, sdk_setup.sh. You can also use the script to generate a response file for a silent installation and to perform a silent installation. When you run sdk_setup.sh, you specify the appropriate options depending on the functions you want to perform.

The following options are available:

-a *response_file*

Creates only a response file with the specified name. This response file can be used for a later installation of the SDK runtime environment.

-F

Forces the installation, ignoring backup errors. When updating an existing installation, sdk_setup.sh first backs up the existing installation in case the update fails. Typically, if the backup fails, the update cannot occur. However, this option instructs the installation to ignore the backup errors and continue with the installation.

-h|-?

Displays the help.

-o

Overlays the response file. This option is used with -a.

-p *log_file*

Logs the installation in the specified file. If the -p option is not specified, the installation log is stored in /opt/CA/installer/log.

-r *response_file*

Installs the SDK runtime environment using the specified response file. Use this option with the –s option.

-s

Installs the SDK runtime environment in unattended (silent) mode. If the-r option is not specified, default parameters are used.

-t *trace_file*

Traces the installation to the specified file.

-v

Displays the version of the installer.

-x

Extracts only the SDK files to the /tmp directory. The file name used for the extracted files is automatically defined and displayed on the command line.

Update the Installation or Reinstall the SDK Runtime Environment

You can update the installation or reinstall the CA Workload Automation AE SDK runtime environment using the installation wizard.

To update the installation or reinstall the SDK runtime environment

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following commands to start the installation process:

   ```
   cd SDK
   ./sdk_setup.sh
   ```

   The Welcome page appears.
4. Select Update/Reinstall and click Next.

   The Active Components page appears if a CA Workload Automation AE component or a dependant CA Common Service is active.
5. Click Next to shut down the active processes.

   Note: Before you can update the installation or reinstall a component, all dependent CA products must be shut down.

   The Review Settings page appears, listing the default settings.
6. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the update completes, the Update Complete page appears.
7. Click Finish.

   The reinstallation is complete.

Remove the SDK Runtime Environment Using sdk_setup.sh

If you no longer need the SDK runtime environment, you can remove it using the installation wizard.

To remove the SDK runtime environment using sdk_setup.sh

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following commands:

   ```
   cd SDK
   ./sdk_setup.sh
   ```

4. Select Remove and click Next.

   The Remove Product page appears.

5. Select the Backup the CA Workload Automation AE SDK and restore the old version if the removal fails check box and click Next.

   The Review Removal Settings page appears, listing the default settings.

6. Review the information and, if it is correct, click Remove.

   The Uninstallation Complete page appears.

7. Click OK.

   The SDK runtime environment is removed.

Remove the SDK Runtime Environment Using lsm

If you no longer need the SDK runtime environment, you can remove it using the lsm command.

To remove the SDK runtime environment using the lsm command

1. Log in as root.
2. Run the following command:

   ```
   ./lsm –e CAWorkloadAutomationAE-SDK
   ```

3. When you are prompted to continue with the removal, type y.

   The SDK runtime environment is removed.

Chapter 10: Installing the Server, Client, or Agent Silently

This chapter describes how to perform unattended (silent) installations of CA Workload Automation AE.

This section contains the following topics:

How to Install the Server, Client, or Agent Silently

Alternatively, you can install the server, client, or agent silently, in which case, you are not prompted to manually enter responses like you are during a normal installation. Silent installation uses a response file that you create to automatically provide the required information.

To complete the silent installation, follow these steps:

1. Create a response file (see page 149).
2. Install the server, client, or agent silently (see page 150).

Create a Response File

A response file provides responses to the prompts that occur when you perform a silent installation. You can create a response file by running the interview portion of the installation. You can then use the response file to install the server, client, or agent silently on a computer.

Note: The server, client, or agent will not be installed when you are creating the response file.

To create a response file

1. Log in as root.
2. Mount the CA Workload Automation AE media.

3. Change directories to the mounted file system and run the following command:

   `./wa_setup.sh –a response_file`

   response_file

   Defines the name of the response file. You must include the full path and the path must reference a writable file system.

   The Welcome page appears.

4. Click Next.

   The License Agreement page appears.

5. Read the license text. When you have scrolled to the bottom of the license text, the I Agree button is enabled. If you agree with the license agreement, click I Agree.

   Note: If you click I Disagree, you cannot continue with the installation.

   The Installation Type page appears.

6. Continue with the installation by entering the required information on each page, and clicking Next.

   The Review Settings page appears after the last data entry page, listing the settings you chose for the response file.

7. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   A response file is created.

Install the Server, Client, or Agent Silently

Silent installation lets you install the server, client, or agent without having to enter responses to the prompts. Instead, silent installation uses your previously-created response file to provide the required information.

To install the server, client, or agent silently, run the following command:

`./wa_setup.sh -s -r response_file`

response_file

Specifies the name of an existing response file. You must include the full path.

The server, client, or agent is installed silently.

Chapter 11: Post-Installation Procedures for the Server

This chapter describes the tasks you can perform to customize CA Workload Automation AE after it has been installed.

This section contains the following topics:

Startup Scripts

CA Workload Automation AE creates the following scripts to start the agent, application server, and scheduler at system startup:

`waae_agent-`*`WA_AGENT`*
`waae_sched.$AUTOSERV`
`waae_server.$AUTOSERV`

WA_AGENT

Specifies the name of the agent assigned during installation. The default is WA_AGENT.

$AUTOSERV is the instance name. These scripts are active if you select the corresponding options in the setup wizard.

The scripts are located in the following directories:

- /etc/init.d (on Linux and Solaris)
- /sbin/init.d (on HP-UX)
- /etc/rc.d (on AIX)

Each script accepts the conventional start or stop argument. The root user can run these scripts to start or stop the CA Workload Automation AE services manually. For example, the following script starts the *WA_AGENT* agent and instance ACE's application server on a Linux computer:

```
/etc/init.d/waae_agent-WA_AGENT start
/etc/init.d/waae_server.ACE start
```

The database must be available for the application server and scheduler to start. If CA Workload Automation AE uses an Oracle or Sybase database on the same computer, you can start the application server and scheduler at startup only if you start the database first.

More information:

Start the Scheduler (see page 90)
Start the Application Server (see page 91)

Default EDIT and EXEC Superusers

The *EDIT superuser* is the only user who can change the database password and remote authentication method, change the owner of a job, or edit any job regardless of who owns it.

The *EXEC superuser* is the only user who has permissions to stop the scheduler. The EXEC superuser can also start and stop all jobs, regardless of their ownership or permissions.

By default, the EDIT and EXEC superusers are assigned to one of the following user accounts:

- The owner account of the CA Workload Automation AE product files (if the account exists or you selected the Create the owner and group account option during the installation)
- root (if the owner account does not exist or was not created during installation)

Define Additional EDIT and EXEC Superusers

After installation, you can define additional EDIT and EXEC superusers.

To define additional EDIT and EXEC superusers

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   autosys_secure
   ```

   The following menu appears:

   ```
   Please select from the following options:
   [1] Activate EEM instance security.
   [2] Manage EDIT/EXEC superusers.
   [3] Change database password.
   [4] Change remote authentication method.
   [5] Manage user@host users.
   [6] Get Encrypted Password.
   [0] Exit CA WAAE Security Utility.
   >
   ```

3. Enter 2 and press the Enter key.

   The Manage EDIT/EXEC superusers menu appears.

4. Enter 1 and press the Enter key.

   The Create an EDIT superuser and Create an EXEC superuser prompts appear.

5. Enter the EDIT superuser name and domain.

   The EDIT superuser is created and the following message appears:

   ```
   CAUAJM_I_60069 User successfully added.
   ```

6. Enter the EXEC superuser name and domain.

   The EXEC superuser is created and the following message appears:

   ```
   CAUAJM_I_60069 User successfully added.
   ```

   Note: The EDIT and EXEC privileges can be assigned to the same user. These users must be valid users on the computer or domain that you are logged on to. At this time, you need to enter the host or domain for the user. However, a superuser name without a host or domain name is still supported.

7. Enter 0.

   You exit from the autosys_secure command. The data is loaded into the database.

Notes:

- The Manage EDIT/EXEC superusers menu is only available when autosys_secure is first run and option 2 is selected. After the superusers are modified for the first time, only the EDIT superuser can access this menu. When this menu is accessed again, the current settings are displayed. The EDIT superuser can accept the same users by pressing Enter, or change the users by entering a new specification.
- For more information about the autosys_secure command, see the *Reference Guide*.

Database Tracking

You can run the autotrack command to set your appropriate database tracking level. The autotrack command tracks changes to the database (for example, job definition changes, sendevent calls, and job overrides) and writes this information to the database. Changes to job definitions made through the command utilities can be tracked. Changes made directly to the database through SQL statements cannot be tracked.

When you query for this information, the autotrack command prints a report to the screen, or you can redirect the output to a file.

Automatic tracking is useful for the following:

- Sites that require monitoring of the job definition environment.
- Sites where multiple users have permission to edit job definitions or send events.

Set Up the Database Tracking Level

You can run the autotrack command to set your appropriate database tracking level.

To set up the database tracking level, issue the following command:

```
autotrack –u 0|1|2
```

0

Does not track changes to the database. This is the default.

1

Tracks changes to the database and condenses each tracked event to a one-line summary.

2

Tracks the same information as level 1, but also writes the entire job definition for overrides and job definition changes.

Note: This level is database-intensive and significantly impairs JIL performance.

The database tracking level is set.

Note: For more information about the autotrack command, see the *Reference Guide*.

Configure the Firewall

Firewalls may block the ports CA Workload Automation AE uses to communicate with client utilities and agents that are located outside of the firewall. To prevent communication problems, configure the firewall to accept incoming messages from clients and agents.

Note: Unless otherwise noted, the UNIX parameters listed in the following table are defined in the configuration file, and the Windows fields are located in CA Workload Automation AE Administrator. For more information about the UNIX parameters, see the *Administration Guide*. For more information about the Windows fields, see the *Online Help*.

To configure the firewall, add the following ports as exceptions:

Port	Location on UNIX	Location on Windows
Scheduler auxiliary listening port	SchedAuxiliaryListeningPort parameter	Auxiliary Listening Port field in the Scheduler window of the Administrator utility
Application server auxiliary listening port for all non-SSA communication	AppSrvAuxiliaryListeningPort parameter	Auxiliary Listening Port field in the Application Server window of the Administrator utility
Application server listening port for all SSA communication	AutoServerPort parameter	Client Communication Port field in the Application Server window of the Administrator utility
SSA IANA-defined port (default: 7163)	The PmuxServerPort=*value* displayed by the following command: csamconfigedit display	The PmuxServerPort=*value* displayed by the following command: csamconfigedit display
CA Workload Automation Agent ports	port attribute in all agent machine definitions	port attribute in all agent machine definitions

Port	Location on UNIX	Location on Windows
Legacy agent port	AutoRemPort parameter	Legacy Remote Agent Port field in the Scheduler window of the Administrator utility

Chapter 12: Modifying an Existing Installation

This section contains the following topics:

Update the Installation or Reinstall a Component

If necessary, you can update the installation or reinstall any of the CA Workload Automation AE components (server, client, or agent) using the installation wizard.

To update the installation or reinstall an existing component

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following command to start the installation process:

   ```
   ./wa_setup.sh
   ```

   The Welcome page appears.
4. Select Update/Reinstall and click Next.

   The Active Components page appears if a CA Workload Automation AE component or a dependant CA Common Service is active.
5. Click Next to shut down the active processes.

   Note: Before you can update the installation or reinstall a component, all dependent CA products must be shut down.

   The Review Settings page appears, listing the default settings.

6. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Monitor Progress page appears and the progress is displayed. When the update completes, the Update Complete page appears.

7. Click Finish.

   The reinstallation is complete.

Add New Features to an Installation

After installing CA Workload Automation AE components, you may need to install additional features.

To add new features to an existing installation

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following command:

   ```
   ./wa_setup.sh
   ```

   The Welcome page appears.

4. Select Modify and click Next.

   The Modify Installation Function page appears.

5. Select Add Features and click Next.

   The Components page appears.

6. Select the additional features you want to install, and click Next.
7. Continue with the installation by entering the required information in each wizard page and clicking Next.

   The Review Settings page appears, listing the information you entered.

8. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The new features are installed.

Add a New Instance to an Installation

After installing CA Workload Automation AE components, you may need to add a CA Workload Automation AE instance.

To add a new instance to an existing installation

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following command:

   ```
   ./wa_setup.sh
   ```

   The Welcome page appears.
4. Select Modify and click Next.

   The Modify Installation Function page appears.
5. Select Add Instance and click Next.

   The Add Instance page appears.
6. Enter a name for the new instance and click Next.

   The Data Encryption page appears.
7. Continue with the installation by entering the required information in each wizard page and clicking Next.

   The Review Settings page appears, listing the information you entered.
8. Review the information and, if it is correct, click Next.

   Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

   The Instance Modification Results page appears, showing that a new instance has been added.

Delete an Instance from an Installation

After installing CA Workload Automation AE components, you may need to delete a CA Workload Automation AE instance.

To delete an instance from an existing installation

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following command:

   ```
   ./wa_setup.sh
   ```

4. Select Modify and click Next.

   The Modify Installation Function page appears.

5. Select Delete Instance and click Next.

   The Remove Instance page appears.

6. Select the instance to delete and click Next.

   The Review Settings page appears, listing the instance name you selected.

7. Review the information, and if it is correct, click Next to remove the instance.

   A confirmation message appears that the selected instance is deleted.

Note: If only one instance of CA Workload Automation AE exists, you cannot delete it using this method. You must instead uninstall the product.

Recreate the Oracle Tablespaces or Sybase Database

You can recreate the Oracle tablespaces or Sybase database if the database becomes corrupted. Before recreating the CA Workload Automation AE Oracle tablespaces or Sybase database, verify that you have backed up the existing Oracle tablespaces or Sybase database.

To recreate the Oracle tablespaces or Sybase database

1. Verify that all CA Workload Automation AE components are shut down.
2. Change directories to the following, as appropriate:
   - (Oracle) $AUTOSYS/dbobj/ORA
   - (Sybase) $AUTOSYS/dbobj/SYB

3. Run the following command:

   ./rm_waae_p*ACE*.sh

   ACE

   Specifies the instance that was created when CA Workload Automation AE was installed.

   You will be prompted for the database connection information.

   Note: Default values are supplied based on the installed database type (Oracle or Sybase).

4. Continue by entering the required information at each prompt and pressing Enter.

   The existing CA Workload Automation AE database tables, roles, and users are removed.

   (Sybase only) **Note:** You must remove the Sybase device files, which are in the directory specified in the Sybase Data and Log Directories. For example, if the device files are in /opt/sybase/data, run the following commands:

   ```
   cd /opt/sybase/data
   rm –f AEDB_DATA.DAT
   rm –f AEDB_LOG.DAT
   ```

5. Source the CA Workload Automation AE environment by running the following command:

   ```
   .   ./opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.shell.host
   ```

6. Run the following command:

   ```
   perl ./CreateAEDB.pl
   ```

   You are prompted for information to create the Oracle tablespaces or Sybase database.

Chapter 13: Configuring CA Workload Automation AE to Work with the Agent

This chapter describes optional procedures for configuring CA Workload Automation AE and the agent installed on UNIX, Linux, Windows, or i5/OS.

Note: For information about advanced agent configuration tasks (for example, setting up the agent as an FTP server), or for more details about the agent parameters and security settings, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide*.

This chapter also describes required procedures for configuring CA Workload Automation AE to work with the agent installed on z/OS.

This section contains the following topics:

Configuring for CA WA Agent for UNIX, Linux, Windows, or i5/OS

After you install and define the agent, you can run jobs with that agent. This section describes the optional procedures you can perform to configure CA Workload Automation AE to work with the agent installed on a UNIX, Linux, Windows, or i5/OS computer.

agentparm.txt File

You can configure the agent by editing the parameters in the agentparm.txt file. When you install the agent, the installation program adds commonly-configured agent parameters to the agentparm.txt file. Other agent parameters exist, which you must manually add to the agentparm.txt file to configure the agent. You can modify these parameter values as required.

The agentparm.txt file is located in the following directory:

install_directory/SystemAgent/*agent_name*

install_directory

Specifies the root directory where CA Workload Automation AE is installed.

agent_name

Specifies the name of the agent.

Notes:

- If the agent was installed using a program that was not provided with CA Workload Automation AE (for example, the installation program provided on the CA Workload Automation Agent DVD), the path to the agentparm.txt may be different. In this case, the agentparm.txt file is located in the root directory where the agent is installed.
- For information about the parameters in the agentparm.txt file and how to configure them to work with the scheduling manager, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.*
- When you make a change to an agent parameter that is also defined on CA Workload Automation AE, such as the agent name, you must configure the corresponding parameter on CA Workload Automation AE. Similarly, when you configure an agent parameter on CA Workload Automation AE, the agentparm.txt file must be updated to include the change.

More Information:

Configure Agent Parameters (see page 170)

How the Agent Connects to the CA Workload Automation AE Instance

The agent stores the connection properties of the CA Workload Automation AE instance that it works with in the agent's agentparm.txt file using the following parameters:

- communication.managerid_*n*
- communication.manageraddress_*n*
- communication.managerport_*n*
- communication.socket_*n*

These parameters are automatically updated when CA Workload Automation AE sends a message to the agent. You do not have to modify these parameters.

However, when you define the agent as a machine to the CA Workload Automation AE instance, you must specify the following agent properties in the machine definition:

- Agent name—Specifies the name of the agent. This value must match the agentname parameter in the agentparm.txt file.
- Agent port—Specifies the port of the agent. This value must match the communication.inputport parameter in the agentparm.txt file.
- Encryption key—Specifies the path to the cryptkey.txt file that stores the encryption key for the agent. This value must match the security.cryptkey parameter in the agentparm.txt file.

You must ensure that these values in the machine definition match the agentparm.txt values. Otherwise, the agent and the CA Workload Automation AE instance cannot communicate.

How to Configure CA Workload Automation AE to Work with the Agent

This topic outlines the general steps that you can perform to configure CA Workload Automation AE to work with an agent. The steps apply to the agent on UNIX, Linux, Windows, or i5/OS.

To configure CA Workload Automation AE to work with the agent, follow these steps:

1. Define the agent on CA Workload Automation AE (see page 117).
2. Define a user on CA Workload Automation AE (see page 166).
3. Setting up security permissions on CA Workload Automation AE (see page 167).
4. (Optional for i5/OS only) Run UNIX workload on a System i5 computer.
5. Verify that the agent works with CA Workload Automation AE (see page 120).

More Information:

Agents and Agent Plug-ins (see page 19)

Define a User on CA Workload Automation AE

To run jobs on an agent computer, you must define user IDs and passwords that the jobs will run under.

Notes:

- On UNIX, we recommend that you use the root account to run a job on the agent computer. Using the root account lets you run jobs under different user accounts. For more information about running jobs under a specific user account, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.*
- You can define a default user ID in the agentparm.txt file so that all jobs on the agent computer run under the default user ID. For more information about defining a default user ID, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide*.
- You must define user IDs and passwords on CA Workload Automation AE for Database, FTP, PeopleSoft, or SAP jobs. You do not need to define user IDs and passwords on CA Workload Automation AE for Oracle jobs or Command jobs on UNIX.

To define a user on CA Workload Automation AE

1. Log on to CA Workload Automation AE as the EDIT superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   autosys_secure
   ```

   The following menu appears:

   ```
   Please select from the following options:
   [1] Activate EEM instance security.
   [2] Manage EDIT/EXEC superusers.
   [3] Change database password.
   [4] Change remote authentication method.
   [5] Manage user@host users.
   [6] Get Encrypted Password.
   [0] Exit CA WAAE Security Utility.
   ```

3. Enter 5 and press the Enter key.

   The following menu appears:

   ```
   Please select from the following options:
   [1] Create user@host or Domain password.
   [2] Change user@host or Domain password.
   [3] Delete user@host or Domain password.
   [4] Show all user@host users.
   [9] Exit from "Manage user@host users" menu.
   [0] Exit CA WAAE Security Utility.
   ```

4. Enter 1 and press the Enter key.
5. Enter the user name, user host or domain, and the password when prompted.

   The user is added. The following message appears:

   ```
   CAUAJM_I_60135 User create successful.
   ```

Setting Up Security Permissions on CA Workload Automation AE

You must set up the following security permissions on CA Workload Automation AE to control agent access:

- Permission to run work on the agent—By defining the agent using the insert_machine subcommand and specifying that agent in the job definition.
- Permission to run a job on the agent under a user ID—By defining the user IDs and passwords using the autosys_secure command.
- Permission for the agent to control which CA Workload Automation AE user IDs can perform FTP transfers or submit jobs under a specific agent user ID—The security.txt file contains the local security rules that allow or deny the CA Workload Automation AE user IDs the authority to perform FTP transfers or submit jobs under a specific agent user ID.

  Note: For more information about the security.txt file and setting up local security on the agent, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.* The following agent local security rules described in the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide* do not apply to CA Workload Automation AE:

  - The following security rule that controls which scheduling manager user IDs can issue control commands and send messages to an agent:

    ```
    c a | d manager_userID CONTROL command
    ```

  - The following security rule that controls which users are allowed to submit jobs on behalf of other users:

    ```
    x a | d manager_userID agent_userID path
    ```

    On CA Workload Automation AE, jobs are always submitted to run under the user specified in the owner attribute. If local security is enabled on the agent, the agent checks the permissions of the job owner only. The agent does *not* check the CA Workload Automation AE user who submits the job. Therefore, if local security is enabled on the agent, you can define security rules as follows:

    ```
    x a | d job_owner agent_userID path
    ```

More Information:

Define the Agent on CA Workload Automation AE (see page 117)
Define a User on CA Workload Automation AE (see page 166)

Modify the Encryption Type and Encryption Key on CA Workload Automation AE

You can specify the encryption type and encryption key to be used for each agent during the agent installation. However, after you install the agent, you can modify the encryption type and the encryption key using the encryption_type and key_to_agent JIL attributes. On the agent, the encryption key is stored in the cryptkey.txt file, which is located in the agent installation directory. The security.cryptkey parameter in the agentparm.txt file specifies the path to the cryptkey.txt file.

To modify the encryption type and encryption key on CA Workload Automation AE

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   `unisrvcntr stop waae_agent-`*`WA_AGENT`*

   WA_AGENT

   Defines the name of the agent to stop.

   The agent stops.
3. Enter **jil** at the operating system prompt.

   The JIL command prompt is displayed for the local CA Workload Automation AE instance.
4. Enter the following commands:

   `update_machine:` *`machine_name`*
   `agent_name:` *`agent_name`*
   `encryption_type: NONE | DEFAULT | AES`
   `key_to_agent:` *`key`*

   machine_name

   Specifies the name of the agent to update.

   agent_name

   Specifies the name of an agent.

   NONE | DEFAULT | AES

   Specifies the type of encryption to be used by the agent. You can set the encryption type to *one* of the following:

   NONE

   Specifies that the agent uses no encryption.

   DEFAULT

   Specifies that the agent uses the default encryption key and type. This is the default.

AES

Specifies that the agent uses AES 128-bit encryption.

Note: You must specify a key using the key_to_agent attribute.

key

Specifies the key used to encrypt data from CA Workload Automation AE to the agent. This value must match the security.cryptkey parameter in the agent's agentparm.txt file, without the prefix 0x. If the values do not match, CA Workload Automation AE cannot communicate with the agent. You must specify *one* of the following:

- A 32-digit hexadecimal key
- A passphrase with up to 16 characters

5. Enter exit.

   The data is loaded into the database.

6. If you specify the encryption type as NONE, open the agentparm.txt file, set the security.cryptkey parameter to no value as follows, and save the file:

   ```
   security.cryptkey=
   ```

7. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start waae_agent-WA_AGENT
   ```

   WA_AGENT

   Defines the name of the agent to start.

   The agent starts. The encryption key is modified on CA Workload Automation AE.

Example: Define a User-specific Encryption Key on CA Workload Automation AE

This example defines a user-specific encryption key on CA Workload Automation AE. The encryption key you specify must match the encryption key specified in the cryptkey.txt file.

```
update_machine: machine3
agent_name: WA_MACH3
node_name: machine3
encryption_type: AES
key_to_agent: 0x000102030405060708090A0B0C0D0E0Fl
```

More Information:

agentparm.txt File (see page 163)

Configure Agent Parameters

When you make a change to an agent parameter in the agentparm.txt file that is also defined on CA Workload Automation AE, such as the agent name, you must configure the agent parameter on CA Workload Automation AE.

To configure agent parameters

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   `unisrvcntr stop waae_agent-`*`WA_AGENT`*

   WA_AGENT

   Defines the name of the agent to stop.

   The agent stops.
3. Open the agentparm.txt file located in the agent installation directory.
4. Edit the parameters to make the required changes.
5. Save and close the agentparm.txt file.
6. Enter **jil** at the operating system prompt.

   The JIL command prompt is displayed for the local CA Workload Automation AE instance.
7. Enter the following commands to make the same changes on CA Workload Automation AE:

   ```
   update_machine: machine_name
   agent_name: agent_name
   port: port_number
   max_load: load_units
   factor: real_number
   encryption_type: NONE | DEFAULT | AES
   key_to_agent: key
   heartbeat_attempts: number_of_signals
   heartbeat_freq: minutes
   ```

   machine_name

   Specifies the name of the agent to update.

   agent_name

   (Optional) Specifies the name of an agent.

   Default: WA_AGENT

   port_number

   (Optional) Specifies the port that the agent uses to listen for traffic.

   Default: 7520

load_units

(Optional) Defines how many load units are allowed on the agent simultaneously. This number can be any value in the user-defined range of possible values. The range is also arbitrary.

real_number

(Optional) Defines a real number from a user selected range of values.

Default: 1.0

NONE | DEFAULT | AES

(Optional) Specifies the type of encryption to be used by the agent. You can set the encryption type to *one* of the following:

NONE

Specifies that the agent uses no encryption.

DEFAULT

Specifies that the agent uses the default encryption key and type. This is the default.

AES

Specifies that the agent uses AES 128-bit encryption.

Note: You must specify a key using the key_to_agent attribute.

key

(Optional) Specifies the key used to encrypt data from CA Workload Automation AE to the agent. This value must match the security.cryptkey parameter in the agent's agentparm.txt file, without the prefix 0x. If the values do not match, CA Workload Automation AE cannot communicate with the agent. You must specify *one* of the following:

- A 32-digit hexadecimal key
- A passphrase with up to 16 characters

number_of_signals

(Optional) Specifies the number of heartbeat signals the scheduler tries to detect before it sends an SNMP message indicating inactivity.

Default: 1

minutes

(Optional) Specifies how frequently the scheduler sends the heartbeat signal (in minutes).

Default: 5

8. Enter exit.

   The data is loaded into the database.

9. If you specify the encryption type as NONE, open the agentparm.txt file, set the security.cryptkey parameter to no value as follows, and save the file:

   ```
   security.cryptkey=
   ```

10. Enter the following command at the operating system prompt:

    ```
    unisrvcntr start waae_agent-WA_AGENT
    ```

    WA_AGENT

    Defines the name of the agent to start.

    The agent starts. The agent parameters are configured.

Note: For more information about the update_machine subcommand, see the *Reference Guide*.

Example: Configure the Agent Name on CA Workload Automation AE

Suppose that you want to change the agent name to WA_MACH2. You must edit the agentname parameter in the agentparm.txt file to WA_MACH2 and enter the following commands at the operating system prompt:

```
update_machine: machine1
agent_name: WA_MACH2
```

Note: You must stop and restart the agent for the changes to take effect.

More Information:

agentparm.txt File (see page 163)

Configure the Agent to Communicate with CA Workload Automation AE

You can configure the agent to communicate with CA Workload Automation AE by editing or adding the communication parameters in the agentparm.txt file.

Notes:

- You can configure the agent to work with multiple scheduling managers by adding additional definitions in the agentparm.txt file.
- You must add the following parameter to the agentparm.txt file to configure the agent to communicate with CA Workload Automation AE that supports Internet Protocol version 6 (IPv6) and dual Internet Protocol (dual IP) environments:

  `java.net.preferIPv6Addresses=true`
- On HP-UX, you must add the following parameter to the agentparm.txt file to enable IPv6 on Java.

  `java.net.preferIPv4Stack=false`

To configure the agent to communicate with CA Workload Automation AE

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   `unisrvcntr stop waae_agent-`*`WA_AGENT`*

   WA_AGENT

   Defines the name of the agent to stop.

   The agent stops.
3. Open the agentparm.txt file located in the agent installation directory.
4. Edit or add the communication parameters as appropriate, and save the file.
5. Enter the following command at the operating system prompt:

   `unisrvcntr start waae_agent-`*`WA_AGENT`*

   WA_AGENT

   Defines the name of the agent to start.

   The agent starts, and is configured to communicate with CA Workload Automation AE.

Example: Configure the Agent to Communicate with CA Workload Automation AE

This example shows the configuration parameters that are set in the agentparm.txt file for the CA Workload Automation AE instance “ACE” at address 172.31.255.255. CA Workload Automation AE listens for incoming messages from the agent on port 7500:

```
communication.manageraddress_1=172.31.255.255
communication.managerid_1=ACE_SCH
communication.managerport_1=7500
communication.inputport=7520
communication.receiver.socket.main=plain
communication.socket_1=plain
communication.single_connection_attempts_1=1
communication.single_connection_hold_1=100
```

Communication Parameters in the agentparm.txt File

When the scheduler communicates with the agent, the communication parameters are added to the agentparm.txt file.

The communication parameters are added to the agentparm.txt file in the following situations:

- When you issue the autoping command or run client utilities, such as the jil and autorep commands.
- When you start the scheduler or the application server.

Note: The agentparm.txt file includes the communication parameters corresponding to all the CA Workload Automation AE instances that communicate with the agent.

The following communication parameters are added to the agentparm.txt file:

communication.manageraddress_1

Defines the IP address or host name of CA Workload Automation AE that the agent works with. You can specify a list of addresses for CA Workload Automation AE.

Example: 172.24.36.107 (IPv4) or 0:0:0:0:0:FFFF:192.168.00.00 (IPv6)

Notes:

- The communication.manageraddress_1 value specified in the agentparm.txt file must match the AutoServer parameter value in the configuration file. For more information about the AutoServer parameter, see the *Administration Guide*.
- You can specify a DNS name instead of the IP address for CA Workload Automation AE. However, your agent computer must be able to resolve the DNS name at all times. If there is a DNS outage and your agent computer cannot resolve DNS names, the agent cannot communicate with CA Workload Automation AE.
- If the CA Workload Automation AE IP address never changes, enter the DNS name for CA Workload Automation AE in your agent computer's hosts file. This entry helps ensure that the IP address can be resolved after DNS disruptions.

communication.managerid_1

Specifies the name of the CA Workload Automation AE instance that the agent works with.

Default: *instance*_SCH

Example: ACE_SCH

Note: The communication.managerid_1 value specified in the agentparm.txt file must match the AutoServerId parameter value in the configuration file. For more information about the AutoServerId parameter, see the *Administration Guide*.

communication.managerport_1

Specifies the port that CA Workload Automation AE listens on for communication from agents. The valid port range is 1024-65534.

Note: The communication.managerport_1 value specified in the agentparm.txt file must match the AutoServerPort or AppSrvAuxiliaryListeningPort parameter value in the configuration file. For more information about the AutoServerPort or AppSrvAuxiliaryListeningPort parameters, see the *Administration Guide*.

communication.inputport

(Optional) Specifies the main port number the agent uses to listen for incoming messages from CA Workload Automation AE.

Default: 7520

Limits: 1024-65534

Note: On UNIX, ports 1–1023 are reserved ports and require root access.

communication.single_connection_attempts_1

Specifies the number of times to check if the transmitter queue contains data to send.

communication.single_connection_hold_1

Specifies the time (in milliseconds) to hold the connection between checks after the last message is sent.

communication.socket_1

Defines the socket type the agent and CA Workload Automation AE use for communication. The following socket types are available:

- plain
- dylan

Default: plain

Optional Communication Parameters

You can add the following optional communication parameters to the agentparm.txt file to configure the communication between CA Workload Automation AE and the agent:

communication.inputport.aux

(Optional) Specifies the auxiliary port number the agent uses to listen for incoming messages from CA Workload Automation AE.

communication.receiver.socket.aux

(Optional) Specifies the type of socket the agent uses for its auxiliary port. The value of this parameter must be different than the communication.receiver.socket.main parameter. You can specify the following socket types:

- plain
- dylan

communication.receiver.socket.main

(Optional) Specifies the type of socket the agent uses for its main port. The value of this parameter must be different than the communication.receiver.socket.aux parameter. You can specify the following socket types:

- plain
- dylan

Default: plain

Note: If you are using the agent with two scheduling managers that require different socket types for communication, you can specify a main and auxiliary socket for the agent.

How to Configure the Agent to Communicate Using SSA Ports

Notes:

- This procedure only applies to agents that communicate with CA Workload Automation AE using SSA ports.
- By default the agent uses plain socket ports for communication. Although you can change to SSA communication, we do not recommend it.

SSA lets CA Workload Automation AE and the agent use a single multiplexed communication port to ease firewall administration.

To configure the agent to communicate using SSA ports, follow these steps:

1. Configure the agent to communicate using an SSA-enabled port (see page 178).
2. Define the agent SSA port on CA Workload Automation AE (see page 179).
3. Test communication between CA Workload Automation AE and the agent (see page 121).

Configure the Agent to Communicate Using an SSA-Enabled Port

By default, the agent is configured to use plain socket ports for communication. You can use the csamconfigedit utility (installed with SSA) to enable SSA communication between the agent and CA Workload Automation AE.

Important! The port number defined in the machine definition for the agent must match the communication.inputport parameter in the agentparm.txt file.

To configure the agent to communicate using an SSA-enabled port

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   unisrvcntr stop CA-WAAE
   ```

   The scheduler, application server, and the agent stop.
3. Enter the following command at the operating system prompt:

   ```
   csampmux stop
   ```

   The csampmuxf process stops.
4. Change to the $CSAM_SOCKADAPTER/bin directory, and enter the following command at the operating system prompt:

   ```
   csamconfigedit Port=value EnableSSL=False EnablePmux=True
   ```

   value

   Specifies the SSA port number of the agent. This port must not be used by another application.

   Note: The CA Workload Automation AE installer automatically configures SSA to register 49154-50176 as virtual ports. These ports are known as the *ephemeral port range* and are used for short-term communications for application server, scheduler, and the agent.
5. Open the agentparm.txt file located in the agent installation directory.

6. Edit the following parameters, and save the file:

   ```
   communication.inputport=port
   communication.receiver.socket.main=dylan
   oscomponent.classpath=jars/*.jar:jars/ext/*:common_components_installation_path/Csam/SockAdapter/lib/casocket.jar
   ```

   port

   Specifies the SSA port number configured using the csamconfigedit command.

   common_components_installation_path

   Specifies the path to the directory where the CA common components are installed.

   Default: /opt/CA/SharedComponents

   Note: Append the location of the casocket.jar file to the classpath to specify the location of SSA.

7. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start CA-WAAE
   ```

   The scheduler, application server, and the agent start. The agent is configured to communicate using an SSA-enabled port.

More Information:

agentparm.txt File (see page 163)

Define the Agent SSA Port on CA Workload Automation AE

To communicate with the agent using an SSA-enabled port, you must change the port defined in the machine definition for the agent on CA Workload Automation AE.

To define the agent SSA port on CA Workload Automation AE

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter **jil** at the operating system prompt.

   The JIL command prompt is displayed for the local CA Workload Automation AE instance.

3. Enter *one* of the following subcommands:

   - If you are creating a new agent machine definition:

     `insert_machine: machine_name`

   - If you are updating an existing agent machine definition:

     `update_machine: machine_name`

   machine_name

   Defines a unique name for the agent. When defining jobs, specify this name in the machine attribute.

4. Specify the following attribute:

   `port: port_number`

   port_number

   Specifies the port that the agent uses to listen for traffic. If you configured SSA on the agent, this value is the agent port number configured using the csamconfigedit command. This value must match the communication.input port parameter in the agentparm.txt file for the agent.

   The SSA port is defined in the machine definition for the agent on CA Workload Automation AE.

Run UNIX Workload on a System i5 Computer

CA WA Agent for i5/OS lets you schedule jobs on the i5/OS operating system. In addition to scheduling native i5/OS jobs, you can schedule most UNIX workload, such as UNIX scripts, in the PASE environment on i5/OS.

To run both native and UNIX jobs on the same i5/OS computer, you must install two CA WA Agents for i5/OS on that computer. On the agent that runs native i5/OS jobs, set the following parameter in the agentparm.txt file:

```
oscomponent.targetenvironment=I5
```

On the agent that runs UNIX jobs, set the following parameter in the agentparm.txt file:

```
oscomponent.targetenvironment=UNX
```

Notes:

- For more information about setting the oscomponent.targetenvironment parameter, see the *CA Workload Automation Agent for i5/OS Implementation Guide*.
- For more information about UNIX workload that can run in the PASE environment, see the IBM i5/OS documentation.

Configuring for CA WA Agent for z/OS

After you install the agent on z/OS, you must perform additional configuration tasks on CA Workload Automation AE and the agent so that they can communicate with each other. After you perform these tasks, you can define and run jobs on the mainframe.

AGENTDEF Data Set

You can configure the agent on z/OS by editing the parameters in the AGENTDEF data set. The parameter values in the AGENTDEF data set are set during the agent installation. You can modify these parameter values as required.

Notes:

- For information about the parameters in the AGENTDEF data set and how to configure them to work with the scheduling manager, see the *CA Workload Automation Agent for z/OS Installation and Configuration Guide*.
- When you make a change to an agent parameter that is also defined on CA Workload Automation AE, such as the agent name, you must configure the corresponding parameter on CA Workload Automation AE. Similarly, when you configure an agent parameter on CA Workload Automation AE, the AGENTDEF data set must be updated to include the change.

More Information:

Configure the AGENTDEF Data Set on the Agent on z/OS (see page 189)

Encryption Between CA Workload Automation AE and the Agent on z/OS

Depending on the encryption types that the agent on z/OS supports, data can be transferred between CA Workload Automation AE and the agent with no encryption or with AES 128-bit encryption. The encryption settings on CA Workload Automation AE and the agent must match.

Encryption occurs in two ways:

- The data received from the agent
- The data sent to the agent

Encryption of Data Received from the Agent on z/OS

The encryption setting for CA Workload Automation AE is determined as follows:

- On UNIX—By the UseCommAliasEncryption parameter in the configuration file.
- On Windows—By the Use AES 128-bit encryption when communicating with zOS managers check box under the zOS Encryption tab on the Instance - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.

CA Workload Automation AE uses no encryption or AES 128-bit encryption to exchange data with the agent on z/OS. If you are using AES encryption, you must generate an instance-wide communication alias encryption file (cryptkey_alias.txt) in the $AUTOUSER.*instance_name* (on UNIX) or %AUTOUSER%.*instance_name* (on Windows) directory. The cryptkey_alias.txt file stores the communication alias encryption key. CA Workload Automation AE expects the agent on z/OS to encrypt the data using the key specified in the cryptkey_alias.txt file.

If you are using no encryption, CA Workload Automation AE expects the data it receives from the agent on z/OS to be unencrypted.

Important! You must set AES encryption only if AES encryption is also configured on the agent on z/OS. For more information about the encryption types that the agent on z/OS supports, see the CA WA Agent for z/OS documentation.

Notes:

- The current release of CA WA Agent for z/OS is r2.0. This release of the agent does not support AES 128-bit encryption. To run z/OS jobs using this agent, you must disable AES 128-bit encryption and use no encryption for z/OS communication.
- If CA Workload Automation AE works with other agents on z/OS, the administrator must update all AGENTDEF data sets with the encryption setting.

Example: Using No Encryption When Receiving Data from the Agent on z/OS

Suppose that you do not want the data received from the agent on z/OS to be encrypted. To use no encryption, you must set the UseCommAliasEncryption parameter to 0 in the configuration file (on UNIX) or clear the Use AES 128-bit encryption when communicating with zOS managers check box under the zOS Encryption tab on the Instance - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator (on Windows).

When you define your CA Workload Automation AE instance to the agent, you must specify the NOENCRYPT operand, as follows:

```
COMMCHAN instancename_AGT ADDRESS(address) PORT(sched_aux_port) -
UNIX ASCII TCPIP PREF(2) NOENCRYPT
EXTSCHED AUTO SAFUSER(user) EVENTPREFIX(prefix) -
APPLPREFIX(ZOS) MAXACTIVE(3) ID(agent_name)
```

More information:

Configure the AGENTDEF Data Set on CA Workload Automation EE (see page 243)

Encryption of Data Sent to the Agent on z/OS

The encryption setting for the agent on z/OS is determined by the ZOSAGENT initialization parameter in the AGENTDEF data set, as shown in the following example:

```
ZOSAGENT NAME(manager_name) TCPIP
```

In this example, the ENCRYPT operand is excluded from the parameter, so no encryption is used. The agent expects the data it receives from CA Workload Automation AE to be unencrypted.

If encryption is specified in the ZOSAGENT parameter, the agent expects CA Workload Automation AE to encrypt the data.

Important! On CA Workload Automation AE, you must specify the same agent encryption setting using the encryption_type and key_to_agent attributes. Therefore, to use encryption, the agent on z/OS and CA Workload Automation AE must support the same encryption type. For more information about the encryption types that the agent on z/OS supports, see the CA WA Agent for z/OS documentation.

Example: Using No Encryption to Send Data to the Agent on z/OS

Suppose that agent on z/OS does not need the data transferred to be encrypted. To use no encryption, the ENCRYPT operand is excluded from the ZOSAGENT initialization parameter of the AGENTDEF data set, as follows:

```
ZOSAGENT NAME(manager_name) TCPIP
```

When you define the agent on z/OS to CA Workload Automation AE, you must specify the encryption_type: NONE attribute, as follows:

```
insert_machine: machine_name
type: a
opsys: zos
node_name: address
agent_name: agent_name
port: port_number
encryption_type : NONE
```

More information:

Configure the AGENTDEF Data Set on CA Workload Automation EE (see page 243)

How to Configure CA Workload Automation AE to Work with the Agent on z/OS

CA WA Agent for z/OS submits and tracks z/OS jobs.

To configure CA Workload Automation AE to work with the agent on z/OS, follow these steps:

1. Configure the scheduler and application server auxiliary listening ports (see page 184).
2. Define a unique communication alias for the application server (see page 186).
3. Set encryption for z/OS communication (see page 187).
4. (AES 128-bit encryption only) Generate an instance-wide communication alias encryption file (see page 188).
5. Configure the AGENTDEF data set on the agent on z/OS (see page 189).
6. Define the agent on z/OS on CA Workload Automation AE (see page 191).
7. Verify that the agent on z/OS works with CA Workload Automation AE (see page 120).

Configure the Scheduler and Application Server Auxiliary Listening Ports

The scheduler and the application server communicate with CA Workload Automation EE and CA WA Agent for z/OS using non-SSA ports. Therefore, you must disable port multiplexing and SSL encryption for the scheduler and application server auxiliary listening ports.

Note: If the ports are already configured, skip this procedure.

To configure the scheduler and application server auxiliary listening ports

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Edit the following parameters in the configuration file as follows, and save the file:

   `SchedAuxiliaryListeningPort=`*`sch_port`*

   sch_port

   Defines the port number the scheduler uses to communicate with CA Workload Automation EE and the agent on z/OS. This port is used for all non-SSA communication.

   `AppSrvAuxiliaryListeningPort=`*`appsrv_port`*

appsrv_port

Defines the port number the application server uses to communicate with CA Workload Automation EE and the agent on z/OS. This port is used for all non-SSA communication.

The scheduler and application server auxiliary listening ports are defined.

3. Enter the following commands at the operating system prompt:

```
cd $CSAM_SOCKADAPTER/bin
csamconfigedit Port=sch_port EnableSSL=False EnablePmux=False
```

sch_port

Specifies the port number to configure. You must specify the same scheduler auxiliary listening port that you specified in the SchedAuxiliaryListeningPort parameter in the configuration file.

Port multiplexing and SSL encryption are disabled for the specified scheduler auxiliary listening port.

4. Enter the following command at the operating system prompt:

```
csamconfigedit Port=appsrv_port EnableSSL=False EnablePmux=False
```

appsrv_port

Specifies the port number to configure. You must specify the same application server auxiliary listening port that you specified in the AppSrvAuxiliaryListeningPort parameter in the configuration file.

Port multiplexing and SSL encryption are disabled for the specified application server auxiliary listening port.

5. Enter the following commands at the operating system prompt:

```
unisrvcntr stop waae_sched.$AUTOSERV
unisrvcntr stop waae_server.$AUTOSERV
```

The scheduler and the application server stop.

6. Enter the following command at the operating system prompt:

```
csampmux stop
```

The csampmuxf process stops.

7. Enter the following commands at the operating system prompt:

```
unisrvcntr start waae_sched.$AUTOSERV
unisrvcntr start waae_server.$AUTOSERV
```

The scheduler and the application server start. The scheduler and application server auxiliary listening ports are configured.

Note: For more information about the SchedAuxiliaryListeningPort and AppSrvAuxiliaryListeningPort parameters, see the *Administration Guide*.

Define a Unique Communication Alias for an Application Server

The application server requires an additional communication alias to communicate with CA WA Agent for z/OS. The communication alias is set to *INSTANCENAME_ABBREVIATEDHOSTNAME* during the CA Workload Automation AE installation.

If the CA Workload Automation AE instance has multiple application servers, the communication alias for each application server must be unique. If an alias is not unique, you must define another alias for that application server.

Note: The scheduler also requires a communication alias to communicate with the agent on z/OS. However, the communication alias for the scheduler is automatically set to *INSTANCENAME*_AGT (in uppercase). You cannot change this value.

To define a unique communication alias for an application server

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   unisrvcntr stop waae_server.$AUTOSERV
   ```

   The application server stops.
3. Edit the following parameter in the configuration file as follows, and save the file:

   ```
   AutoServerAliasId=unique_alias
   ```

   unique_alias

   Defines a unique communication alias that the application server uses to communicate with the agent on z/OS.

   Default: *INSTANCENAME_ABBREVIATEDHOSTNAME*. The abbreviated hostname consists of the last 12 characters of the node name excluding the domain name. For example, the communication alias of the application server on myhost.ca.com is set to ACE_MYHOST, where ACE is the name of the CA Workload Automation AE instance.

   Limits: Up to 16 uppercase characters

   Note: If you specify the value in lowercase or mixed case, the value is automatically changed to uppercase.
4. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start waae_server.$AUTOSERV
   ```

   The application server starts. The unique communication alias is defined for the application server. The application server uses this alias to communicate with the agent on z/OS.

Set Encryption for z/OS Communication on UNIX

CA Workload Automation AE uses no encryption or AES 128-bit encryption to exchange data with CA Workload Automation EE and CA WA Agent for z/OS. If you are using AES encryption, you must generate an instance-wide communication alias encryption file (cryptkey_alias.txt) in the $AUTOUSER.*instance_name* (on UNIX) or %AUTOUSER%.*instance_name* (on Windows) directory. The cryptkey_alias.txt file stores the communication alias encryption key.

Important! You must set AES encryption for z/OS communication only if AES encryption is also configured on CA Workload Automation EE or the agent on z/OS. For more information about the encryption types that CA Workload Automation EE and the agent on z/OS support, see the CA Workload Automation EE and CA WA Agent for z/OS documentation.

Notes:

- The current release of CA WA Agent for z/OS is r2.0. This release of the agent does not support AES 128-bit encryption. To run z/OS jobs using this agent, you must disable AES 128-bit encryption and use no encryption for z/OS communication. To disable AES encryption, you must set the UseCommAliasEncryption parameter to 0 in the configuration file.
- If CA Workload Automation AE works with other CA Workload Automation EE external instances or the agents on z/OS, the administrator must update all AGENTDEF data sets with the encryption setting.

To set encryption for z/OS communication on UNIX

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following commands at the operating system prompt:

   ```
   unisrvcntr stop waae_sched.$AUTOSERV
   unisrvcntr stop waae_server.$AUTOSERV
   ```

   The scheduler and the application server stop.

3. Edit the following parameter in the configuration file, and save the file:

   `UseCommAliasEncryption=0|2`

   0

   Specifies that no encryption is used.

   2

   Specifies that AES encryption is used to encrypt data.

   Note: If you set the UseCommAliasEncryption parameter to 2, you must generate the cryptkey_alias.txt file and specify the communication alias encryption key using the -a option of the as_config command.

4. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start waae_sched.$AUTOSERV
   unisrvcntr start waae_server.$AUTOSERV
   ```

   The scheduler and the application server start. The encryption for z/OS communication is set.

Notes:

- For information about specifying the encryption key using the as_config command, see the *Reference Guide*.
- On Windows, you can select the equivalent value using the Use AES 128-bit encryption when communicating with zOS managers check box under the zOS Encryption tab on the Instance - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator. For information about setting encryption for z/OS communication on Windows, see the *Online Help* or the *Windows Implementation Guide*.

Generate an Instance-Wide Communication Alias Encryption File

CA Workload Automation AE uses no encryption or AES 128-bit encryption to exchange data with CA Workload Automation EE and CA WA Agent for z/OS. If you are using AES encryption, you must generate the instance-wide communication alias encryption file (cryptkey_alias.txt).

The cryptkey_alias.txt file stores the communication alias encryption key. The cryptkey_alias.txt file is located in the $AUTOUSER.*instance_name* (on UNIX) or %AUTOUSER%.*instance_name* (on Windows) directory.

Important! Do this procedure only if AES encryption is also configured on CA Workload Automation EE or the agent on z/OS. For more information about the encryption types that CA Workload Automation EE and the agent on z/OS support, see the CA Workload Automation EE and CA WA Agent for z/OS documentation.

Notes:

- A CA Workload Automation AE instance can have only one cryptkey_alias.txt file. Before you do this procedure, check whether the file already exists. If the file exists, skip this procedure. You must provide the key associated with that file to the CA Workload Automation EE or agent administrator. They need the key to configure the AGENTDEF data set.
- If you do not know the key associated with the existing cryptkey_alias.txt, you can regenerate the file using a new key. If CA Workload Automation AE works with other CA Workload Automation EE external instances or the agents on z/OS, the administrator must update all AGENTDEF data sets with the new key.

To generate an instance-wide communication alias encryption file

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   `as_config -a key`

   key

   Specifies the communication alias encryption key. You must prefix the hexadecimal identifier 0x to this value.

   Limits: Must contain 32 characters; valid characters are 0-9 and A-F.

   Note: This key must match the key stored in the ENCRYPT KEYNAME(*keyname*) parameter in the AGENTDEF data set of CA Workload Automation EE or the agent on z/OS.

   The communication alias encryption file (cryptkey_alias.txt) is generated with the encryption key. AES 128-bit encryption is used.

Configure the AGENTDEF Data Set on the Agent on z/OS

For communication to occur between CA Workload Automation AE and the agent on z/OS, you must configure the AGENTDEF data set on the agent on z/OS. The parameters in the AGENTDEF data set must match the settings defined on CA Workload Automation AE.

To configure the AGENTDEF data set, add the following entries:

```
COMMCHAN INSTANCENAME_AGT ADDRESS(sch_ip_address) PORT(sch_aux_port) platform +
ASCII TCPIP PREF(2) encryption_setting
```

```
COMMCHAN AutoServerAliasId ADDRESS(appsrv_ip_address) PORT(appsrv_aux_port) +
platform ASCII TCPIP PREF(2) encryption_setting
```

The following table describes the operands that are not self-explanatory and their corresponding CA Workload Automation AE settings:

AGENTDEF Operand	Description	Corresponding CA Workload Automation AE Setting
COMMCHAN *INSTANCENAME*_AGT	Specifies the name associated with the encryption data between CA Workload Automation AE and the agent on z/OS.	*INSTANCENAME*_AGT This is the communication alias for the CA Workload Automation AE scheduler. The value must be in uppercase. *INSTANCENAME* is the name of the CA Workload Automation AE instance.
COMMCHAN *AutoServerAliasId*	Specifies the name associated with the encryption data between CA Workload Automation AE and the agent on z/OS.	AutoServerAliasId parameter in the configuration file.
ADDRESS(*sch_ip_address*)	Specifies the host name or the IP address of the computer where the CA Workload Automation AE scheduler is installed.	None
ADDRESS(*appsrv_ip_address*)	Specifies the host name or the IP address of the computer where the CA Workload Automation AE application server is installed.	None
PORT(*sch_aux_port*)	Specifies the port number that the CA Workload Automation AE scheduler uses for all non-SSA communication.	SchedAuxiliaryListeningPort parameter in the configuration file.
PORT(*appsrv_aux_port*)	Specifies the port number that the CA Workload Automation AE application server uses for all non-SSA communication.	AppSrvAuxiliaryListeningPort parameter in the configuration file.
platform	Specifies whether the CA Workload Automation AE instance is installed on UNIX or Windows. Options are UNIX or NT.	None

AGENTDEF Operand	Description	Corresponding CA Workload Automation AE Setting
encryption_setting	Specifies the type of encryption used.	If encryption is *not* configured on the agent, encryption_type: NONE must be defined in the machine definition, and the cryptkey_alias.txt file must not exist. If encryption is configured on the agent, encryption_type: AES must be defined in the machine definition. The same key must be stored in the cryptkey_alias.txt file in the $AUTOUSER.*instance_name* directory. **Note:** To use encryption, both the agent on z/OS and CA Workload Automation AE must support AES encryption. For more information about the encryption types that the agent supports and how to specify the encryption setting, see the CA WA Agent for z/OS documentation.

Note: For more information about the AGENTDEF data set on the agent on z/OS, see the *CA Workload Automation Agent for z/OS Installation and Configuration Guide*.

More Information:

AGENTDEF Data Set (see page 181)

Define the Agent on z/OS on CA Workload Automation AE

You must define the agent on z/OS on CA Workload Automation AE to enable communication between the agent and the server.

You must ensure that the parameters you specify when you define the agent on z/OS on CA Workload Automation AE match the corresponding parameters in the AGENTDEF data set.

To define the agent on z/OS on CA Workload Automation AE

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter **jil** at the operating system prompt.

   The JIL command prompt is displayed for the local CA Workload Automation AE instance.

3. Enter the following commands:

```
insert_machine: machine_name
type: a
node_name: address
agent_name: agent_name
port: port_number
encryption_type: NONE | AES
```

machine_name

Defines a unique name for the agent on z/OS. When defining jobs, specify this name in the machine attribute.

a

Specifies that the machine is a CA Workload Automation Agent for UNIX, Linux, Windows, i5/OS, or z/OS.

address

(Optional) Defines the IP address or DNS name of the computer where the agent on z/OS is installed.

Default: The value specified in the insert_machine: *machine_name* command.

Note: If you do not specify the node_name attribute, insert_machine: *machine_name* (the default) must be the DNS name of the agent machine. Otherwise, CA Workload Automation AE cannot connect to the agent on z/OS.

agent_name

(Optional) Specifies the name of the agent on z/OS.

Default: WA_AGENT

Note: This name must match the ZOSAGENT(name) parameter in the AGENTDEF data set (on CA WA Agent for z/OS).

port_number

(Optional) Specifies the port that the agent on z/OS uses to listen for traffic.

Default: 7520

Note: This port number must match the COMMCHAN PORT(port) parameter in the AGENTDEF data set (on CA WA Agent for z/OS).

NONE | AES

(Optional) Specifies the type of encryption to be used by the agent on z/OS. You can set the encryption type to *one* of the following:

NONE

Specifies that the agent on z/OS uses no encryption.

AES

Specifies that the agent on z/OS uses AES 128-bit encryption.

Note: You must generate the instance-wide communication alias encryption file (cryptkey_alias.txt) using the as-config command.

Note: To use encryption, both the agent on z/OS and CA Workload Automation AE must support AES encryption. You must specify the same CA Workload Automation AE encryption setting in the AGENTDEF data set of the agent. For more information about the encryption types that the agent supports, see the CA WA Agent for z/OS documentation.

4. (Optional) Specify optional machine attributes:
   - character_code
   - description
   - opsys
   - max_load
   - factor
   - heartbeat_attempts
   - heartbeat_freq
5. Enter exit.

   The data is loaded into the database. The agent on z/OS is defined on CA Workload Automation AE.

Notes:

- For more information about the insert_machine subcommand and the related machine attributes, see the *Reference Guide*.
- For more information about the AGENTDEF data set on the agent on z/OS, see the *CA Workload Automation Agent for z/OS Installation and Configuration Guide*.

Example: Define the agent on z/OS on CA Workload Automation AE

This example defines the agent on z/OS on CA Workload Automation AE.

```
insert_machine: zagent113
type: a
opsys: zos
port: 7520
encryption_type: NONE
character_code: EBCDIC
```

How to Verify the Agent on z/OS Works With CA Workload Automation AE

You can verify communication between the agent on z/OS and CA Workload Automation AE by defining, running, and monitoring a test job.

To verify the agent on z/OS works with CA Workload Automation AE, follow these steps:

1. Test communication between CA Workload Automation AE and the agent (see page 121).
2. Define a z/OS job (see page 194).
3. Run the test job (see page 122).
4. Monitor the test job (see page 123).

Define a z/OS Job

You can define a z/OS job to test communication between CA Workload Automation AE and the agent on z/OS.

To define a z/OS job

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter **jil** at the operating system prompt.

   The JIL command prompt is displayed for the local CA Workload Automation AE instance.
3. Enter the following commands:

   ```
   insert_job: job_name
   job_type: ZOS
   machine: machine_name
   jcl_library: library
   jcl_member: member
   owner: user@host
   ```

   A z/OS job is defined. The following message appears:

   ```
   CAUAJM_I_50323 Inserting/Updating job: job_name
   CAUAJM_I_50205 Database Change WAS Successful!
   ```
4. Enter exit.

   The data is loaded into the database.

Chapter 14: Configuring CA Workload Automation AE to Work with CA Common Components

This section contains the following topics:

CA Embedded Entitlements Manager (CA EEM)

CA Workload Automation AE includes features that let you secure objects such as jobs, calendars, cycles, global variables, machines, and resources. You can delegate administrative privileges to these objects to specific users or user groups. CA Workload Automation AE provides security in the following ways:

- System-level security
- Native security
- External security

External security is enabled by integrating CA Workload Automation AE with CA EEM. The external security mode is robust and provides better flexibility than the native security mode.

An EDIT superuser can enable external security by using the autosys_secure command. When external security mode is enabled, CA EEM is used to assign administrative rights to a user to define policies and to check whether a given user can switch the security mode of CA Workload Automation AE back to native. CA EEM lets you manage your user base, create roles for your enterprise, and assign roles to users. It also maintains security policies that govern what objects can be accessed by which users.

Note: While external security mode is enabled, native security is not enforced. For more information about system-level security, native security, or external security, see the *CA Workload Automation Security Guide*.

Event Management

You can integrate CA Workload Automation AE with Event Management to automate manual problem resolution tasks, filter and consolidate multiple events, monitor for unusual conditions, and take proper corrective action.

The Event Management system collects events from running programs or scripts that generate them and provides a complete view of the ongoing processing in your enterprise. Event Management checks which messages are important and responds to them based on user-defined policies.

With Event Management, you can do the following:

- Identify events that are important to your organization and define message record and action profiles that specify the special processing that CA NSM performs when the events occur.
- Define calendars that set dates and times for processing events.
- Monitor event activity through the console log and immediately respond to events as they occur.
- Define console log views that restrict message access to authorized users and user groups.

How Event Manager Processes Events

In the context of Event Management, an *event* is a message that an operating system or other application issues to alert the user or other software components of an important occurrence. Information, such as date, time, node of origin, and user, is typically associated with the event.

A typical event goes through the following stages:

1. A situation or an event occurs that causes the creation of a message. The message can be informational, such as announcing that a job is completed. It can also announce a more serious event, such as a server going down.
2. The event is sent directly to the Event Manager or collected by various components and sent to the Event Manager for processing.
3. The event is added to the console log if a message policy does not prevent it from being added.
4. The event is matched against one or more Event Management message policies and Advanced Event Correlation (AEC) policies and various actions are executed automatically. Depending on the policy, the event can also go to the Held Messages area of the console log or to Alert Management System (AMS) for further tracking and processing.

5. When human intervention is required, a technician is notified by the Notification Services component of CA NSM. The technician then starts to resolve the situation. If the event was a held message, the technician also acknowledges the message or sends a reply.
6. The situation that caused the message is resolved, and another event can be created to announce the resolution.

Message IDs

You can configure the Event Management Console to restrict the CA Workload Automation AE messages that are forwarded to the focal point system based on the message ID. All the CA Workload Automation AE messages begin with the string %CAATS_ or %CAUAJM_. The subsequent character indicates whether the message is informational, a warning, or an error.

For CA Workload Automation AE, the message prefixes are as follows:

%CAUAJM_I

Indicates an informational message.

%CAUAJM_W

Indicates a warning message.

%CAUAJM_E

Indicates an error message.

Another underscore follows the message type indicator, and then the three remaining characters in the message ID represent a three-digit message number.

Note: For information about how to take full advantage of the Event Management Console to view these messages, see the *Unicenter Network and Systems Management Inside Event Management and Alert Management Guide*.

How to Integrate CA Workload Automation AE with Event Management

This topic provides an overview of the steps that you must perform to integrate CA Workload Automation AE with Event Management.

To integrate CA Workload Automation AE with Event Management, follow these steps:

1. Install an Event Agent on the CA Workload Automation AE server from the CA Common Components DVD (shipped with CA Workload Automation AE) or CA NSM media.

   Notes:

   - If you select only the Event Agent during the installation, check that you already have an Event Manager installed in your enterprise and that you know the name of the Event Manager node. The CA common components installation prompts you for the computer name of the Event Manager node.
   - The Event Agent requires a valid CAICCI connection to the Event Manager computer if the manager is not installed locally on the CA Workload Automation AE server computer.

2. Configure message forwarding (see page 199).

UNIX Integration Considerations

The following are important considerations when you integrate CA Workload Automation AE with Event Management on UNIX:

- The CA Common Components installation records the Event Manager node in the following environment variables that are located in the $CAIGLBL0000/scripts/envset file:
  - CAI_OPR_REMOTEDB
  - CAI_CAL_REMOTEDB
  - CA_CAL_SYSTEMID
- To redefine the manager on systems running CA NSM, you must modify the data in the Event Management environment variables (CAI_OPR_REMOTEDB, CAI_CAL_REMOTEDB, and CA_CAL_SYSTEMID) and recycle CA NSM.
- If you modify the environment variables, you must stop and start the Event Agent using the unishutdown all and unistart all commands to implement your changes.

- If you install only the Event Agent, the Event Management environment variables specify the manager from which the Event Agent retrieves its policies. No messages are forwarded to the manager or any other location unless it is specified in a policy defined for this Event Agent. The policy resides on the manager as a Message Record defined for the Event Agent node with a FORWARD action of the complete message text, where the forwarding destination is the manager node. After the policy is defined and reloaded on the manager and the Event Agent is recycled to pick up the new policy, all messages that arrive on the Event Agent are sent to that managing node.
- To make sure that messages are properly forwarded from the Event Agent residing on the CA Workload Automation AE server, do the following:

  1. Make sure that the Event Management environment variables are set to the Event Manager node on the Event Agent computer.
  2. Define a Message Record/Action for the Event Agent node that forwards all messages that occur on the Event Agent computer to the Event Manager node. If the Event Manager is active, issue the opreload command to cause a reload of all new event policies.

Note: For more information about Event Management setup and configuration, see the *Unicenter Network and Systems Management Inside Event Management and Alert Management Guide*.

Configure Message Forwarding

After installing and configuring Event Management, you must configure the CA Workload Automation AE server to activate its message forwarding interface so that messages are forwarded to the Event Management console.

Note: CA Workload Automation AE requires Event Management r11 or r11.2.

To configure message forwarding

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   unisrvcntr stop waae_sched.$AUTOSERV
   ```

   The scheduler completes any processing it is currently performing and stops.

3. Edit the following parameter in the configuration file, and save the file:

   `UnicenterEvents=1|0`

   1

   Specifies that the CA Workload Automation AE messages are forwarded to the Event Management console.

   0

   Specifies that the CA Workload Automation AE messages are not forwarded to the Event Management console. This is the default.

   Note: On Windows, you can select the equivalent value using the Forward all CA WAAE Messages check box on the Integration - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.

   All CA Workload Automation AE messages are forwarded to the Event Management console.

4. Enter the following command at the operating system prompt:

   `unisrvcntr start waae_sched.$AUTOSERV`

   The scheduler starts. Any messages written to the scheduler log now also appear in the Event Management console.

Note: You can write Event Management policies to act on any or all forwarded messages from CA Workload Automation AE. For information about writing and implementing Event Management policies, see the *Unicenter Network and Systems Management Inside Event Management and Alert Management Guide*.

CA Secure Socket Adapter (SSA)

SSA is an application that lets CA components use a single multiplexed communication port to ease firewall administration and minimize conflicts with other applications.

SSA consists of a Connection Broker that receives incoming connections from the physical port and redirects it to the corresponding network application (such as CA Workload Automation AE) that is listening on a virtual port. Similarly, the Connection Broker redirects all outgoing connections sent by network applications using different virtual ports through the same physical port. The Connection Broker must recognize the virtual ports to redirect network traffic to the correct application.

SSA is installed automatically during the CA Workload Automation AE installation. During installation, CA Workload Automation AE configures the default virtual ports it intends to use. However, you can configure CA Workload Automation AE to listen on a different virtual port.

SSA provides the following features:

- Port multiplexing (PMUX)—Increases security and the efficient use of physical ports available on any given host by restricting all CA Workload Automation AE traffic to a single physical port. The only exception is CAICCI, which is not PMUX-enabled and uses its own physical ports, the agent, scheduler, and application server auxiliary ports.

  Notes:

  - If port multiplexing is enabled, CA Workload Automation AE uses virtual ports and traffic through those ports is restricted to a single physical port named *PmuxServerPort*. The default value is 7163 and is set during the CA Workload Automation AE installation. We recommend that you do not change the PmuxServerPort value; however if you want to enable other ports after the CA Workload Automation AE installation, you must configure those additional ports.
  - To accommodate port multiplexing, CA Workload Automation AE uses a daemon broker process named *csampmuxf*. You do not need to start the csampmuxf process because it starts automatically with the first CA Workload Automation AE binary.
  - The virtual ports can have only one process bound to them. The bound process is generally considered a tcp-server. Any number of remote or local clients can connect to the tcp-server process bound to a port.

- Secure Sockets Layer (SSL)—Provides an added layer of protection by encrypting network data before transmitting it over the network. SSL also decrypts the data upon receipt. By default, CA Workload Automation AE is not SSL-enabled.

Important! The PMUX and SSL settings on the CA Workload Automation AE server and clients (such as the jil and autorep commands and SDKs) must match. If CA Workload Automation AE has PMUX or SSL enabled, its clients must also have PMUX or SSL enabled. If PMUX or SSL encryption is turned on for any server process, it must be turned on for all client and server processes that communicate with it. CA Workload Automation AE processes depend on the PMUX and SSL settings of the host.

By default, the agents use plain socket ports to communicate with CA Workload Automation AE. They do not use SSA ports. However, agents that have been configured to use SSA PMUX and SSL setting must also follow these requirements. This includes Unicenter AutoSys JM r11 legacy agents.

The csamconfigedit Command—Configure the Port Settings

CA Workload Automation AE listens to incoming data using virtual ports. SSA redirects the data sent and received from the virtual ports to a single physical port.

The csamconfigedit command lets you configure the settings for the port used by CA Workload Automation AE. This command is located in the bin directory that is referenced by the CSAM_SOCKADAPTER environment variable.

Notes:

- SSA is installed and configured automatically during the CA Workload Automation AE installation. After installation, you can configure the ports that CA Workload Automation AE listens to. To change the port numbers or the settings of existing ports, you must use the csamconfigedit command. Before you configure the ports, you must stop the CA Workload Automation AE processes and the csampmuxf process on all hosts. You must ensure that the port settings must be the same on both the client and server processes.
- This topic explains only those csamconfigedit command parameters that are used to configure the port settings used by CA Workload Automation AE. The SSA configuration settings must be the same on both the client and server processes.

This command has the following format when used to configure CA Workload Automation AE:

- To specify a port number to configure:

  ```
  csamconfigedit Port[=value] [display|delete] [EnablePmux=True|False]
  [EnableSSL=True|False] [PmuxConnectionTimeout=value]
  ```

- To specify a range of port values to configure:

  ```
  csamconfigedit PortRange=49152-50176 [display|delete] [EnablePmux=True|False]
  [EnableSSL=True|False] [PmuxConnectionTimeout=value]
  ```

- To display the command help:

  ```
  csamconfigedit usage
  ```

Port[=*value*]

Defines the port number to configure.

PortRange=49152-50176

Specifies the range of port values to configure. You cannot change this value.

Note: CA Workload Automation AE uses only a few ports in this range. These ports are virtual because port multiplexing is enabled by default (recommended). If you virtualize these ports, any processes other than CA Workload Automation AE processes that are using these ports are not affected.

display|delete

Displays or deletes the current configuration settings of the port or port range.

EnablePmux=True|False

(Optional) Enables port multiplexing.

Default: True

Note: If EnablePmux is set to True, CA Workload Automation AE uses virtual ports provided by SSA. If EnablePmux is set to False, CA Workload Automation AE runs on physical ports.

EnableSSL=True|False

Enables SSL encryption.

Default: False

Notes:

- To successfully communicate with Unicenter AutoSys JM r11 (scheduling jobs and exchanging cross-instance dependencies) the AES encryption must be set to NONE or OFF. To secure message transport within the CA Workload Automation AE r11.3 environment and to Unicenter AutoSys JM r11, we recommend that you enable SSL encryption (EnableSSL=True). If your environment consists of instances that all support AES 128-bit encryption, you do not need to use SSA's SSL encryption. If you enable SSL encryption and are using AES 128-bit instance-wide encryption, the message payload is encrypted twice (once at the application level using AES 128-bit instance-wide encryption and again in the messaging layer using SSL encryption). This incurs additional overhead.
- If you enable SSL encryption (EnableSSL=True), you can also specify the following keyword and value:

ServerStyle=Passive|Active|Deny|Negotiate|Mandate

Defines the style that the CA Workload Automation AE clients use to handle incoming SSL connections. It also applies to outward connections in deciding whether the server can override the client's decisions about using SSL. The ServerStyle parameter applies only if port multiplexing is enabled (EnablePmux=True) and is used even if SSL is not enabled (EnableSSL=False). You can set the ServerStyle parameter to *one* of the following values:

Passive

Accepts both SSL and non-SSL connections based on the SSA configuration settings (EnableSSL and EnablePmux). This is the default.

Active

Accepts both the SSL and non-SSL connections, but the SSL connections must have matching authentication methods.

Deny

Accepts non-SSL connections only. All SSL connections are rejected.

Negotiate

Accepts SSL connections only, but the client can select the authentication methods instead of the server.

Mandate

Accepts SSL connections only. If you apply this style, you must enable SSL (EnableSSL=True) and port multiplexing (EnablePmux=True), and the SSA configuration settings must be the same on both the client and server processes.

Example: EnableSSL=True EnablePmux=True ServerStyle=Mandate

Note: When establishing a connection, the client and the server processes are authenticated based on the authentication methods defined in SSA. CA Workload Automation AE uses the default authentication methods that are defined in SSA.

PmuxConnectionTimeout=*value*

Specifies the time (in seconds) the SSA Connection Broker holds a connection for CA Workload Automation AE to accept it. If the demand placed on the CA Workload Automation AE scheduler and its agent is high, we recommend that you set the Connection Broker time-out period to 30 seconds.

Default: 5

usage

Displays the help for the csamconfigedit command.

More Information:

Configure CA Workload Automation AE to Run with SSL (see page 204)
Configure the Application Server to Listen on a Different Virtual Port (see page 207)

Configure CA Workload Automation AE to Run with SSL

Typically, a client process is remote from the server process. However, a client can be on the same computer that hosts a server process. The clients communicate with the servers across operating environments with no additional configuration. By default, CA Workload Automation AE uses AES algorithm to encrypt data and all messages (whether they are local or across the network).

When SSL is enabled, additional overhead incurs at process startup time. Persistent processes (such as the scheduler, application server, and the agent) incur this one-time cost at startup and function normally after. Client processes (such as JIL, autorep, or sendevent), which are not persistent or are invoked repetitively, incur this cost for each time the process is invoked.

Note: To successfully communicate with Unicenter AutoSys JM r11 (scheduling jobs and exchanging cross-instance dependencies) the AES encryption must be set to NONE or OFF. To secure message transport within the CA Workload Automation AE r11.3 environment and to Unicenter AutoSys JM r11, we recommend that you enable SSL encryption (EnableSSL=True). If your environment consists of instances that all support AES 128-bit encryption, you do not need to use SSA's SSL encryption. If you enable SSL encryption and are using AES 128-bit instance-wide encryption, the message payload is encrypted twice (once at the application level using AES 128-bit instance-wide encryption and again in the messaging layer using SSL encryption). This incurs additional overhead.

To configure CA Workload Automation AE to run with SSL

1. Log on to CA Workload Automation AE as the root user and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   unisrvcntr stop CA-WAAE
   ```

   The scheduler, application server, and the agent stop.
3. Enter the following command at the operating system prompt:

   ```
   csampmux stop
   ```

   The csampmuxf process stops.
4. Enter the following commands at the operating system prompt:

   ```
   cd $CSAM_SOCKADAPTER/bin
   csamconfigedit Port=value EnableSSL=True EnablePmux=True display
   ```

   Notes:

   - If you defined an application server port by editing the AutoServerPort parameter in the configuration file, you must use the same port number for Port=*value.* For more information about defining the communication ports for the application server, see the *Administration Guide*.
   - By default, the ServerStyle parameter value is set to Passive. You must specify the ServerStyle parameter if you want to set the value to Mandate.
5. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start CA-WAAE
   ```

   The scheduler, application server, and the agent start. CA Workload Automation AE is configured to run with SSL, and the configuration settings of the port are displayed.

Notes:

- If you run multiple application servers, you must enable each application server with the same settings.
- If you enable an application server port other than the default, you must also consider how you want that port to behave under the PMUX feature and enable it accordingly.
- You must set the same port configurations on both the CA Workload Automation AE server and client to ensure that the two components can communicate.
- If you enable SSL on one host in the CA Workload Automation AE network, you must enable SSL on all the other hosts in the CA Workload Automation AE network. After you enable SSL for a given host, you must stop and start all the CA Workload Automation AE processes on that host. After all hosts are enabled, all CA Workload Automation AE network traffic is encrypted under SSL.

Example: Enable PMUX and SSL for Port 5101

This example enables PMUX and SSL for port 5101.

```
cd $CSAM_SOCKADAPTER/bin
csamconfigedit Port=5101 ServerStyle=Mandate EnablePmux=True EnableSSL=True
```

Example: Enable PMUX and SSL for the Port Range 49152-50176

This example enables PMUX and SSL for the port range 49152-50176.

```
cd $CSAM_SOCKADAPTER/bin
csamconfigedit PortRange=49152-50176 ServerStyle=Mandate EnablePmux=True
EnableSSL=True
```

More Information:

The csamconfigedit Command—Configure the Port Settings (see page 202)

Virtual Ports Used by CA Workload Automation AE

The CA Workload Automation AE application server and the agent require a port to listen for incoming connections. By default, the CA Workload Automation AE installation configures SSA to recognize virtual port 9000 for the application server. You can configure the application server to listen on a different virtual port.

However, for the CA Workload Automation AE application server, scheduler, and the agent to communicate with one another, virtual ports are dynamically assigned values in the 49152–50176 range. This range is known as the *ephemeral port range* and is reserved for short-term communications. The CA Workload Automation AE installation also configures SSA to register the ephemeral port range as virtual ports.

Configure the Application Server to Listen on a Different Virtual Port

You might want to reconfigure the port that the CA Workload Automation AE application server listens to in the following situations:

- Another CA product is using the default virtual port and you want that product to continue using that port.
- You want to enable more than one application server to run on the same host. You must specify a unique virtual port for each application server.

Note: By default, port multiplexing is enabled on CA Workload Automation AE, and the CA Workload Automation AE installation configures SSA to recognize virtual port 9000 for the application server. If you install multiple CA Workload Automation AE instances on the same computer, subsequent installations use incremental virtual port numbers, such as 9001, 9002, and so on.

To configure the application server to listen on a different virtual port

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   unisrvcntr stop CA-WAAE
   ```

   The scheduler, application server, and the agent stop.
3. Enter the following command at the operating system prompt:

   ```
   csampmux stop
   ```

   The csampmuxf process stops.
4. Change to the $CSAM_SOCKADAPTER/bin directory, and enter the following command at the operating system prompt:

   ```
   csamconfigedit Port=value EnablePmux=True
   ```

   value

   Defines the port number to configure.
5. Enter the following command at the operating system prompt:

   ```
   csamconfigedit Port=value display
   ```

   The configuration settings of the specified virtual port are displayed.

6. Set the AutoServerPort parameter to the specified virtual port in the configuration file.
7. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start CA-WAAE
   ```

   The scheduler, application server, and the agent start. A virtual port is defined for the application server. The application server now listens on the specified virtual port.

More Information:

The csamconfigedit Command—Configure the Port Settings (see page 202)

Configure the Connection Broker Time-Out Period

SSA consists of a Connection Broker that receives incoming connections from the physical port and redirects it to the corresponding network application (such as CA Workload Automation AE) that is listening on a virtual port. All the connections to the Connection Broker are managed through the connection queue. Under typical conditions, the Connection Broker hands over the connection to CA Workload Automation AE in 5 seconds (the default). However, under a large load, the Connection Broker queues up the connection requests and is not able to service a connection within the default time-out period, and the connection is broken. As a result, if you are running jobs on an agent that uses SSA ports, you may notice performance issues and connection failures between the CA Workload Automation AE scheduler and the agent. Therefore, to handle large loads, we recommend that you set the Connection Broker time-out period to 30 seconds.

To configure the Connection Broker time-out period

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   ```
   unisrvcntr stop CA-WAAE
   ```

   The scheduler, application server, and the agent stop.
3. Enter the following command at the operating system prompt:

   ```
   csampmux stop
   ```

   The csampmuxf process stops.

4. Change to the $CSAM_SOCKADAPTER/bin directory, and enter the following command at the operating system prompt:

   `csamconfigedit Port=value EnablePmux=True PmuxConnectionTimeout=30`

   value

   Defines the port number to configure.

   30

   Specifies that the SSA Connection Broker time-out period is 30 seconds.

5. Enter the following command at the operating system prompt:

   `unisrvcntr start CA-WAAE`

   The scheduler, application server, and the agent start. The Connection Broker time-out period is set to 30 seconds.

CA, Inc. Common Communications Interface (CAICCI)

CAICCI is the communication layer that lets the CA Workload Automation AE scheduler, which handles cross-platform events, communicate with legacy agents on the distributed, mid-range, and mainframe platforms.

CAICCI consists of several daemon processes and a library. On UNIX, the scheduler communicates with the CAICCI API through the shared library.

On UNIX, CAICCI consists of the following three daemon processes:

caiccid

Builds the CAICCI resources and starts the other two CAICCI daemon processes. Referred to as the main CAICCI daemon because it is started first.

cciclnd

Maintains the CAICCI Inter-Process Communication (IPC) resources. Referred to as the clean daemon process because of that responsibility.

ccirmtd

Transmits data across the network remotely.

ccijimd

Acts as a proxy between CAICCI (multi-threaded application) and CA Workload Automation AE (single-threaded application).

CA Workload Automation AE uses CAICCI to communicate with the following products:

- Event Management
- CA Workload Automation SE
- CA Workload Automation EE
- CA AutoSys WA Connect Option
- CA Jobtrac JM
- CA Scheduler JM

Important Considerations

The following are important considerations about CAICCI:

- You install CAICCI using the CA Common Components DVD.

  Note: For more information about how to install CAICCI, see the *CA Common Components Implementation Guide*.

- CAICCI must be installed on the CA Workload Automation AE server if you want to perform cross-platform scheduling with the following products:
  - CA UJMA
  - CA AutoSys WA Connect Option

Required CAICCI Daemon Processes on UNIX

The following three daemon processes must be running for CAICCI:

```
$ ps -ef|grep cci
root 17733 17731  0   Jan 18 ?       30:36 /uni/cci_kit/cci/bin/ccirmtd
root 17732 17731  0   Jan 18 ?        1:20 /uni/cci_kit/cci/bin/cciclnd
root 17731     1  0   Jan 18 ?        1:25 /uni/cci_kit/cci/bin/caiccid
```

Note: You must have administrator privileges to start or stop CAICCI.

Start CAICCI

After you configure CAICCI, you must start CAICCI for the configuration settings to take effect.

To start CAICCI, run the following script:

```
$CAIGLBL0000/cci/scripts/CA-cci start
```

Note: You must log on as the root user to start or stop CAICCI.

Stop CAICCI

To stop CAICCI, run the following cshut script:

```
$CAIGLBL0000/cci/scripts/cshut
```

Notes:

- You must log on as the root user to start or stop CAICCI.
- If CAICCI stops responding and you cannot shut it down, do the following:

  1. Issue the following command:

     `kill -9 ccirmtd_pid cciclnd_pid caiccid_pid`

     The three CAICCI daemon processes stop running.

  2. Issue the following command:

     `ipcs -a|grep 0000d`

     The shared memory is searched for the caiccid process.

  3. Issue the following command:

     `ipcrm -q message_queue_id`

     The message queue for the caiccid process returned from Step 2 is removed.

  4. Issue the following command:

     `ipcrm -m shared_memory_id`

     The shared memory for the caiccid process returned from Step 2 is removed.

  5. Issue the following command:

     `ipcrm -s semaphore_id`

     The semaphore for the caiccid process returned from Step 2 is removed.

Enable CAICCI Remote Communications

After you install CAICCI, you can use the $CAIGLBL0000/cci/scripts/cci.config script to enable CAICCI remote communications.

To enable CAICCI remote communications

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following commands at the operating system prompt:

   ```
   CCI_RemoteHost=<hostname>; export CCI_RemoteHost
   $CAIGLBL0000/cci/scripts/cci.config
   ```

   The following message appears:

   ```
   During the initial installation, several CCI parameter files were created.
   Do you want to recreate these files as part of this reinstallation?
   (y/n)  (default:  n)
   ```

3. Enter **y**.

   You are prompted for the node names that the CAICCI remote daemon must communicate with, as follows:

   ```
   Please enter the name of the remote host or RETURN to end:
   ```

4. Enter a single node name.

   The prompt is repeated.

5. Enter additional node names, one at a time, until you specified all the node names, and press the Enter key twice.

   CAICCI remote communications are enabled.

caiccid.prf File—Specify Max_Recvrs Value

The caiccid.prf file specifies the Max_Recvrs value and starts the CAICCI clean and remote daemon processes when you start CAICCI.

Note: We recommend that you do not edit the caiccid.prf file, unless the file hits the Max_Recvrs limit.

The caiccid.prf file is located in the following directory:

$CAIGLBL0000/cci/config/*nodename*/caiccid.prf

nodename

Identifies the computer where the CAICCI daemons run.

The caiccid.prf file has the following format:

```
CLN_Demon = cciclnd startup
RMT_Demon = ccirmtd startup
Max_Recvrs = nn,mm
```

cciclnd startup

Starts the CAICCI clean daemon process (cciclnd) when you start CAICCI.

ccirmtd startup

Starts the CAICCI remote daemon process (ccirmtd) when you start CAICCI.

Max_Recvrs = *nn*,*mm*

nn

Defines the number of CAICCI receivers that determine the size of the shared memory segment for RVT lists. This has the effect of limiting the number of application receivers.

Default: 48. You may need to change the default value to match your installation.

Notes:

- Each application requires at least one RVT and each unprocessed CAICCI message requires another RVT. On a busy server, you may need to increase this value to 200 or 300. If the CAICCI_E_FREERVTS error message is displayed in the system log, you must increase this value.
- After you increase this value, asbIII may not start because CAICCI has not started. This sometimes happens because CAICCI must protect access to this shared memory using a semaphore group. CAICCI must create a semaphore group with a semaphore identifier for each RVT plus three extras. On most UNIX platforms, the number of semaphore identifiers in a semaphore group is governed by the SEMMSL kernel parameter. You may need to increase the SEMMSL value. You must ensure that you follow the following rule when increasing this value in the Max_Recvrs parameter:

  SEMMSL >= *nn* + 3

  CAICCI requires two distinct semaphore identifiers at most. If CAICCI gets ID=0, it holds this group and requests another. CA NSM has requirements for XXXMNI, which must be added to the requirements for other products using the IPC resources.

mm

Indicates the number of messages that CAICCI queues up for each application.

Limits: 1-700

Notes:

- The maximum value is 700. However, we recommend specifying 699 as the maximum value because CAICCI shut downs when the 700 buffer is filled to avoid problems with possible limited resources on the local machine, but not for the remote daemon.
- If you set this value to a value higher than the recommended maximum value, it defaults to the maximum.
- Sometimes an application stops responding or is too busy to pick up its messages. In these situations, the following error message is displayed in the system log:

  ```
  CAICCI_E_RECVBUSY Target [ ] queue is full, sender [ ]
  ```

  The application sleeps while it waits for room on the buffer (the default behavior).

Shared Memory for RVTs

Information about a receiver is stored in a structure named *RVT*. Since all applications must have access to this information, it is stored in shared memory as an RVT list. On UNIX, you can view this information by using the cci show command, which produces blocks of data. The first block contains global data and each subsequent block contains information specific to a particular receiver. This information includes the following details:

- The CAICCI address
- The process ID of the application
- Whether the application is ready to accept data or has a message pending.

On UNIX, the caiccid daemon process creates the shared memory segment for RVT lists. When CAICCI starts, it creates the shared memory segment. Therefore, CAICCI must know beforehand how large a memory segment to create.

In addition to storing an application's CAICCI address, the shared memory is used to store the data that the application is sending. Sometimes messages arrive too quickly for the target application to dispose of them. In this scenario, an application may request that CAICCI queues up messages.

ccirmtd.prf File—Identify Local and Remote Parameters

The ccirmtd.prf file identifies the local CAICCI node name, the UNIX host name, and the block size for the local and remote computers.

The ccirmtd.prf file is located in the following directory:

`$CAIGLBL0000/cci/config/nodename/ccirmtd.prf`

nodename

Identifies the computer where the CAICCI daemons run.

The local and remote parameters have the following format:

```
LOCAL = nodename cciname max_msg_size [startup | nostart][port=p retry=x]
REMOTE = nodename cciname max_msg_size [startup | nostart][port=p retry=x]
```

nodename

Defines the host name that is passed to gethostbyname. This value can be any name that can be resolved to the correct IP address and does not require a logical connection to cciname.

cciname

Defines the logical name that CAICCI uses to identify the local host. This name is determined by the ca_uname function during installation and by the ca_nodename function at run time. These functions are the equivalent of uname –n.

Limits: Up to 64 characters

Note: An alias must be used for names with more than eight characters.

max_msg_size

Defines the maximum buffer that CAICCI uses to send or receive messages over the socket. We recommended that you do not edit this value. Each side of the connection may have this set to different values (up to 32 KB). The lesser of the two values is used.

startup | nostart

(Optional) Indicates whether or not to initiate a connection. Sometimes you may only want one side to initiate the connection. Not having the server start connections eliminates a succession of messages when CAICCI is recycled. STARTUP tells CAICCI to attempt a remote connection when activated, whereas NOSTART implies that the remote system will be initiating the connection to the node.

port=*p*

(Optional) Specifies another port for this specific connection only.

Default: 1721

retry=*x*

(Optional) Determines how the ccirmtd daemon process behaves if the connection is dropped. Options are the following:

0

Does not retry the connection.

-1

Starts with a two-second retry interval and doubles after each unsuccessful retry attempt.

n

Waits for *n* seconds between retry attempts, where *n* is any number greater than 0 (zero).

Note: Retry interval is mainly used in conjunction with the nostart option to allow the server to sit passively and wait for incoming connection requests. If a client host goes down, the server will not attempt to reconnect.

Example: Identify Local and Remote Parameters

This example specifies the local and remote parameters.

```
LOCAL = abcdef31 abcdef31 32768 startup
REMOTE = abcdef33 abcdef33 32768 startup
REMOTE = abcdef33 abcdef33 32768 startup port=7000
```

cciclnd.prf File—Define the Time to Sleep Between System Scans

The cciclnd.prf file defines the number of seconds to sleep between system scans for communications buffer and connections cleaning.

Important! The default value is one second. Do not change this value unless instructed by CA Technical Support.

The cciclnd.prf file is located in the following directory:

`$CAIGLBL0000/cci/config/`*`nodename`*`/cciclnd.prf`

nodename

Identifies the computer where the CAICCI daemons run.

CAICCI Environment Variables on UNIX

On UNIX, several CAICCI environment variables are used. You must set these environment variables in the $CAIGLBL0000/cci/scripts/CA-cci file before the main CAICCI daemon process (caiccid) runs, unless otherwise noted.

CAI_CCI_DEBUG Environment Variable

The CAI_CCI_DEBUG environment variable specifies whether the CAICCI traces are enabled or disabled. CAI_CCI_DEBUG affects all processes and applications using CAICCI.

You can use the CAI_CCI_DEBUG environment variable to enable or disable CAICCI traces.

The CAI_CCI_DEBUG environment variable has the following format:

```
CAI_CCI_DEBUG=y|n
```

y

Enables CAICCI traces.

n

Disables CAICCI traces.

CAI_CCI_LOG Environment Variable

The CAI_CCI_LOG environment variable specifies the directory where the CAICCI trace file is written to. CAI_CCI_LOG affects all processes and applications using CAICCI.

You can use the CAI_CCI_LOG environment variable when a larger volume is required for trace output.

The CAI_CCI_LOG environment variable has the following format:

CAI_CCI_LOG=*path*

path

Specifies the directory where the CAICCI trace file is written to.

CAI_CCI_CONFIG Environment Variable

The CAI_CCI_CONFIG environment variable specifies the path to the CAICCI configuration directory. CAI_CCI_CONFIG affects all processes using CAICCI.

You can use the CAI_CCI_CONFIG environment variable to set the path to the CAICCI configuration directory.

The CAI_CCI_CONFIG environment variable has the following format:

`CAI_CCI_CONFIG=`*`path`*

path

Specifies the path to the CAICCI configuration directory. The configuration files are located at $path\–n.

CAI_CCI_SHMMIN Environment Variable

The CAI_CCI_SHMMIN environment variable specifies the minimum size of shared memory segment that CAICCI requests. CAI_CCI_SHMMIN affects all processes and applications using CAICCI.

You can use the CAI_CCI_SHMMIN environment variable when the value of the SHMMIN kernel parameter is greater than 1.

The CAI_CCI_SHMMIN environment variable has the following format:

`CAI_CCI_SHMMIN=`*`SHMMIN`*

SHMMIN

Defines the value of the SHMMIN kernel parameter.

CAI_CCI_PORT1 Environment Variable

The CAI_CCI_PORT1 environment variable specifies the port that the ccirmtd.prf file binds to before connect calls. CAI_CCI_PORT1 affects the remote daemon process.

You can use the CAI_CCI_PORT1 environment variable when there is a firewall or a multi Network Interface Card (NIC) situation.

The CAI_CCI_PORT1 environment variable has the following format:

`CAI_CCI_PORT1=`*`n`*

n

Specifies the port (greater than 256) that the ccirmtd.prf file binds to before connect calls.

CCI_SELECT_TIME Environment Variable

The CCI_SELECT_TIME environment variable determines the time-out period for the TCP/IP handshake to complete. CCI_SELECT_TIME affects the remote daemon process.

You can use the CCI_SELECT_TIME environment variable when the network conditions cause the TCP/IP handshake to take a long time to complete.

The CCI_SELECT_TIME environment variable has the following format:

`CCI_SELECT_TIME=`*n*

n

Determines the time-out period for the TCP/IP handshake to complete. This value must be greater than 1.

Chapter 15: Configuring Cross-Instance Dependencies with CA Workload Automation AE

This section contains the following topics:

CA Workload Automation AE Cross-Instance Job Dependencies

A CA Workload Automation AE *instance* is one licensed version of CA Workload Automation AE software running as a server and as one or more clients, on one or more computers. An instance uses its own scheduler, one or more application servers, and event server, and operates independently of other instances.

Different instances can run from the same executables and can have the same value for $AUTOSYS. However, each instance must have different values for $AUTOUSER and $AUTOSERV. Different instances can also be run on the same computer.

Multiple CA Workload Automation AE instances are not connected, but they can communicate with one another. This communication lets you schedule workload across instances in your enterprise. You can define jobs that have dependencies on jobs running on other instances (*cross-instance job dependencies*). A CA Workload Automation AE job with these dependencies conditionally starts based on the status of the job on the other instance. In this situation, your instance's scheduler acts as a client and issues sendevent commands to the external instance. The other instance's application server processes the sendevent request and stores the dependency request or status update in its database.

You can also manually send events from one instance to another.

CA Workload Automation AE External Instance Type

To use external job dependencies, the scheduling manager or remote machine must be defined as an *external instance* in the CA Workload Automation AE database.

When you define CA Workload Automation AE as an external instance, you must specify the **xtype: a** JIL attribute in the definition. This attribute indicates that the external scheduling manager is a CA Workload Automation AE application server instance.

How to Configure Cross-Instance Dependencies for an r11 or r11.3 Instance

You can create cross-instance job dependencies between your local instance and external CA Workload Automation AE r11 or r11.3 instances. You can also start jobs that are defined on the external instance. Before the instances can communicate with each other, you must configure them.

Note: For information about configuring cross-instance scheduling for r4.5 external instances, see How to Configure Cross-Instance Scheduling for a Unicenter AutoSys JM r4.5 Instance (see page 227).

To configure cross-instance scheduling between your local r11.3 instance and another r11 or r11.3 instance, follow these steps:

1. Do the following:
   a. Define the external r11 or r11.3 instance on the local r11.3 instance (see page 223).
   b. Define the local r11.3 instance on the external r11 or r11.3 instance (see page 224).

   Cross-instance dependencies are configured. You can define jobs on one instance that depends on jobs on the other instance.
2. (Optional) Install a client (see page 98) on the local r11.3 instance.

   Note: When prompted for the Application Server Properties, enter the external r11 or r11.3 instance's application server host name and port number.

   The client is installed and you can issue the sendevent command to start a job on the external r11 or r11.3 instance.

Note: For more information about defining cross-instance jobs and job dependencies, see the *User Guide*.

Define the External r11 or r11.3 Instance on the Local r11.3 Instance

Before the local CA Workload Automation AE r11.3 instance can communicate with an external r11 or r11.3 instance, you must define the external instance on the local instance. All external instance entries are stored in the CA Workload Automation AE event server and can be reported using the autorep command.

To define the external r11 or r11.3 instance on the local r11.3 instance

1. Log on to the local instance and do one of the following:
   - Issue JIL in interactive mode.
   - Open a JIL script in a text editor.
2. Specify the following definition:

   ```
   insert_xinst: external_AE_instance_name
   xtype: a
   xmachine: external_appsrv_host_name[,external_appsrv_host_name2,...]
   xcrypt_type : NONE | DEFAULT | AES
   xkey_to_manager: encryption_key_for_external_instance
   xport: port_number_for_external_appservers
   ```

   Notes:

   - You can specify up to four external application server computers in the xmachine attribute. Separate each external application server computer with a comma.
   - External r11 instances do not support AES encryption. To support external instance job dependencies with r11, AES encryption must be disabled on the local r11.3 instance.
3. Repeat Step 2 for every external instance that you want to communicate with.
4. Do *one* of the following:
   - Enter **exit** if you are using interactive mode.
   - Redirect the script to the jil command if you are using a script.

   The external r11 or r11.3 instance is defined on the local r11.3 instance.

Note: For more information about the JIL attributes, see the *Reference Guide*.

Define the Local r11.3 Instance on the External r11 or r11.3 Instance

You must define the local CA Workload Automation AE r11.3 instance on the external r11 or r11.3 instance so that the external instance can send requests or status updates to it.

To define the local r11.3 instance on the external r11 or r11.3 instance

1. Log on to the external instance and do one of the following:
   - Issue JIL in interactive mode.
   - Open a JIL script in a text editor.
2. Do *one* of the following:
   - If the external instance is r11.3, specify the following definition:

     ```
     insert_xinst: local_AE_instance_name
     xtype: a
     xmachine: local_appserver_host_name[,local_appserver_host_name2,...]
     xcrypt_type : NONE | DEFAULT | AES
     xkey_to_manager: encryption_key_for_local_instance
     xport: port_number_for_local_appservers
     ```

     Note: You can specify up to four local application server computers in the xmachine attribute. Separate each external application server computer with a comma.
   - If the external instance is r11, specify the following definition:

     ```
     insert_xinst: local_AE_instance_name
     xtype: a
     xmachine: host_name\:port
     ```
   - If the external instance is r11 and the local instance uses multiple application servers, add the following attribute for each application server:

     ```
     xmachine: appserver_host_name\:port
     ```

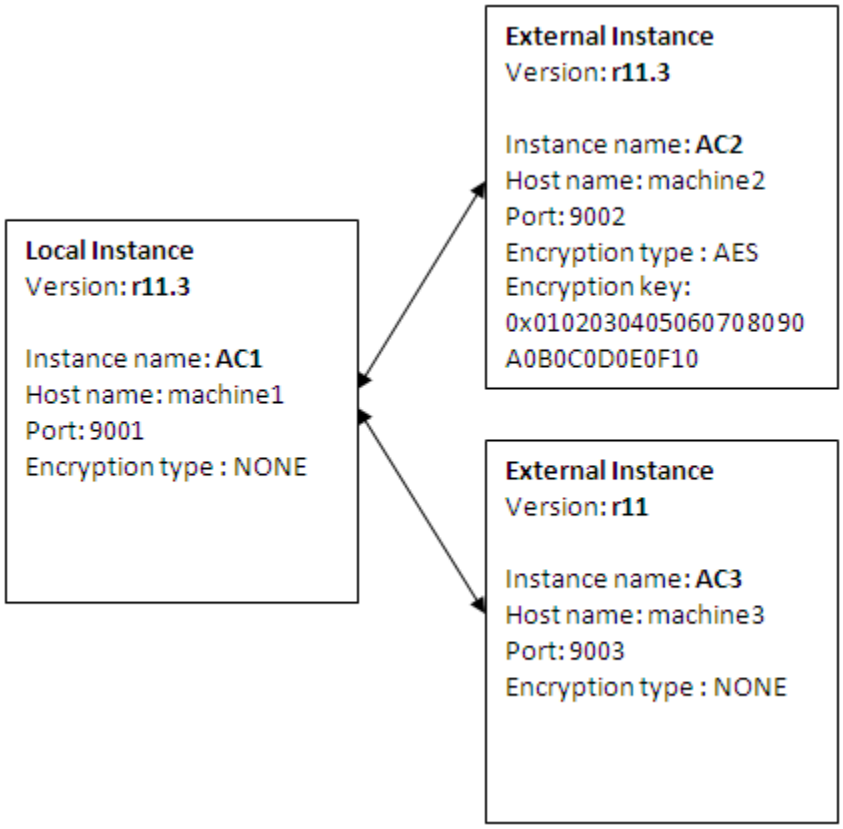
   Note: External r11 instances do not support AES encryption. To support external instance job dependencies with r11, AES encryption must be disabled on the local r11.3 instance.
3. Do *one* of the following:
   - Enter **exit** if you are using interactive mode.
   - Redirect the script to the jil command if you are using a script.

   The local r11.3 instance is defined on the external r11 or r11.3 instance.

Note: For more information about the JIL attributes, see the *Reference Guide*.

Example: Configure Cross-Instance Dependencies for r11.3 and r11 External Instances

Suppose that you want to create cross-instance job dependencies between the following CA Workload Automation AE instances:



To enable communication, you must define the external instances on the local instance and the local instance on the external instances.

On AC1, define the AC2 and AC3 external instances as follows:

```
insert_xinst: AC2
xtype: a
xmachine: machine2
xcrypt_type: AES
xkey_to_manager: 0x0102030405060708090A0B0C0D0E0F10
xport: 9002

insert_xinst: AC3
xtype: a
xmachine: machine3
xcrypt_type: NONE
xport: 9003
```

On AC2, define the AC1 local instance as follows:

```
insert_xinst: AC1
xtype: a
xmachine: machine1
xcrypt_type: NONE
xport: 9001
```

On AC3, define the AC1 local instance as follows:

```
insert_xinst: AC1
xtype: a
xmachine: machine1\:9001
```

AC3 is an r11 external instance and does not support AES encryption. To communicate with AC3, AES encryption cannot be configured on the AC1 r11.3 instance. However, without encryption, AC1 can still communicate with AC2, which is also an r11.3 instance and has AES encryption configured.

Example: Configure Cross-Instance Dependencies for an r11.3 External Instance with Multiple Application Servers

This example configures the local instance to support cross-instance dependencies with an external CA Workload Automation AE r11.3 instance named ACE. One application server for the ACE instance resides on machineA on port 9000. Another application server resides on machineB on port 9000. ACE is defined on the local instance as follows:

```
insert_xinst: ACE
xtype: a
xmachine: machineA,machineB
xcrypt_type: AES
xkey_to_manager: 0102030405060708090A0B0C0D0E0F10
xport: 9000
```

How to Configure Cross-Instance Dependencies for an r4.5 Instance

You can create cross-instance job dependencies between your local r11.3 instance and external Unicenter AutoSys JM r4.5 instances. You can also start jobs that are defined on the external instance. To configure cross-instance dependencies, you must install the r11.3 application server that connects to the event server used by the r4.5 instance and the r4.5 external instance must connect to the event server used by the r11.3 instance. Before the instances can communicate with each other, you must perform a custom server installation, apply the required database patches, and define the external instances.

To configure cross-instance scheduling between your local r11.3 instance and an r4.5 instance, follow these steps:

1. Prepare the r4.5 external instance for cross-instance dependency with an r11.3 instance, as follows:

   a. Install the r11.3 lightweight application server, apply the required database patches, and define the local r11.3 instance on the external r4.5 instance (see page 229).

   b. Run the required SQL statements on the database the external r4.5 instance uses (see page 230).

   Cross-instance dependencies are configured. You can define jobs on one instance that depends on jobs on the other instance.

2. Prepare the r11.3 local instance for cross-instance dependency with an r4.5 instance, as follows:

   a. Apply the required database patches on the local r11.3 instance (see page 231).

   b. Define the external r4.5 instance on the local r11.3 instance (see page 232).

   Cross-instance dependencies are configured. You can define jobs on one instance that depends on jobs on the other instance.

3. (Optional) Install a client (see page 102) on the external r4.5 instance.

   Note: When prompted for the Application Server Properties, enter the external r4.5 instance's application server host name and port number.

   The client is installed and you can issue the sendevent command to start a job on the external r4.5 instance.

   Note: You can issue only the sendevent command on the application server that is connected to the r4.5 event server. The use of other client utilities is not supported.

Note: For more information about defining cross-instance jobs and job dependencies, see the *User Guide*.

Lightweight Application Server

When you install an r11.3 application server and connect it to the event server used by an external r4.5 instance, that application server is named *lightweight application server*. The lightweight application server detects the presence of r4.5 event server data and runs with limited functionality. It processes external dependency and sendevent requests from the local 11.3 instance and writes job events directly into the r4.5 event server.

Note: You can issue only the sendevent command on the application server that is connected to the r4.5 event server. The use of other client utilities is not supported.

Install the r11.3 Lightweight Application Server, Apply the Required Database Patches, and Define the Local r11.3 Instance on the External r4.5 Instance

Before you can start jobs that are defined on an external r4.5 instance or create cross-instance job dependencies, you must apply the required database patches on the event server the external r4.5 instance uses. These database patches create the r11.3 database views and stored procedures that the lightweight application server requires to work with the r4.5 event server.

To install the r11.3 lightweight application server, apply the required database patches, and define the local r11.3 instance on the external r4.5 instance

1. Install the server (see page 85).

   Note: During the server installation, you must do the following:

   - Perform a custom server installation and install only the application server component.
   - The instance name of the application server must match the instance name of the r4.5 instance.
   - Enter the database information for the r4.5 database. Do not select the option to create or refresh the database.

2. Log in to *Download Center*, *Published Solutions* in CA Support Online (http://support.ca.com).
3. Download the following published solution and associated text file, depending on your database type:
   - Microsoft SQL Server—RO03795
   - Oracle—RO03790
   - Sybase—RO03785
4. Follow the instructions in the text file.

   Notes:

   - The instructions apply to r11.3 even though they only indicate r11.
   - For Oracle patch RO03790, you must manually replace all occurrences of MDBADMIN with AEDBADMIN in the sql files.

   The required database patches are applied and the lightweight application server is installed on the external 4.5 instance.

Run the Required SQL Statements on the External r4.5 Instance Database

Before you can start jobs that are defined on external r4.5 instances or create cross-instance job dependencies, you must run the required SQL statements on the event server the external r4.5 instance uses.

To run the required SQL statements on the external r4.5 event server, do *one* of the following (depending on the database type):

- If the database type is Sybase or Microsoft SQL Server 2000 or less, run the following SQL statements on the r4.5 instance database:

```
exec sp_addlogin anyone,anything
go
exec sp_adduser anyone
go
grant select on alamode to anyone
go
```

- If the database type is Microsoft SQL Server 2005 or greater, run the following SQL statements on the r4.5 instance database:

```
CREATE LOGIN anyone WITH PASSWORD = 'anything', CHECK_POLICY = OFF
go
CREATE USER anyone FOR LOGIN anyone
go
grant select on alamode to anyone
go
```

- If the database type is Oracle, run the following SQL statements on the r4.5 instance database:

```
Create user anyone identified by anything;
Grant create session to anyone;
Grant select on alamode to anyone;
```

Apply the Required Database Patches on the Local r11.3 Instance

Before you can start jobs that are defined on an external r4.5 instance or create cross-instance job dependencies, you must apply the required database patches on the event server of the local r11.3 instance. These database patches add the r4.5 database views and stored procedures that the r4.5 scheduler and legacy agent require to work with the r11.3 event server.

To apply the required database patches on the local r11.3 instance

1. Log in to *Download Center*, *Published Solutions* in CA Support Online (http://support.ca.com).
2. Download the following published solution and associated text file, depending on your database type:
   - Microsoft SQL Server—RO03827
   - Oracle—RO03825
   - Sybase—RO03818
3. Follow the instructions in the text file.

   Notes:

   - The instructions apply to r11.3 even though they only indicate r11.
   - For Oracle patch RO03825, you must manually replace all occurrences of MDBADMIN with AEDBADMIN in the sql files.
   - For Microsoft SQL Server patch RO03827 running on Microsoft SQL Server 2005 or greater, you must manually replace the following lines:

     ```
     sp_addlogin 'anyone', 'anything'
     go
     sp_adduser 'anyone', 'anyone'
     go
     ```

     with

     ```
     CREATE LOGIN anyone WITH PASSWORD = 'anything', CHECK_POLICY = OFF
     go
     CREATE USER anyone FOR LOGIN anyone
     go
     ```

   Important! Replace the JIL syntax in Step 5 of the text file with the syntax described in Define the External r4.5 Instance on the Local r11.3 Instance (see page 232).

   The required database patches are applied on the local r11.3 instance.

Define the External r4.5 Instance on the Local r11.3 Instance

Before the local r11.3 instance can communicate with an external r.4.5 instance, you must define the 4.5 instance on the r11.3 instance. All external instance entries are stored in the CA Workload Automation AE event server and can be reported using the autorep command.

To define the external r4.5 instance on the local r11.3 instance

1. Log on to the local r11.3 instance and do one of the following:
   - Issue JIL in interactive mode.
   - Open a JIL script in a text editor.
2. Specify the following definition:

   ```
   insert_xinst: external_AE_r45_instance_name
   xtype: a
   xmachine:
   lightweight_appserver_host_name[,lightweight_appserver_host_name2,...]
   xport: port_number
   xcrypt_type: NONE
   ```

   Notes:
   - You can specify up to four external application server computers in the xmachine attribute. Separate each external application server computer with a comma.
   - External r4.5 instances do not support AES encryption. To support external instance job dependencies with r4.5, the xcrypt_key attribute of the external instance definition must be set to NONE.
3. Repeat Step 2 for every external r4.5 instance that you want to communicate with.
4. Do *one* of the following:
   - Enter **exit** if you are using interactive mode.
   - Redirect the script to the jil command if you are using a script.

   The external r4.5 instance is defined on the local r11.3 instance.

Note: For more information about the JIL attributes, see the *Reference Guide*.

Chapter 16: Configuring Cross-Instance Dependencies with CA Workload Automation EE

This section contains the following topics:

CA Workload Automation EE Job Dependencies

You can define jobs that have cross-instance dependencies on CA Workload Automation EE jobs. A CA Workload Automation AE job with these dependencies conditionally starts based on the status of the job running on the CA Workload Automation EE instance. These dependencies are jobs that execute on an external instance but were not initiated on behalf of the local CA Workload Automation AE instance. When the dependent job completes, status information is sent to the local CA Workload Automation AE instance and recorded in the database.

Note: Bi-directional scheduling is currently not supported between CA Workload Automation AE and CA Workload Automation EE.

CA Workload Automation EE External Instance Type

To use external job dependencies, the scheduling manager or remote machine must be defined as an *external instance* in the CA Workload Automation AE database.

When you define CA Workload Automation EE as an external instance, you must specify **xtype: e** JIL attribute in the definition. This attribute indicates that the external scheduling manager is CA Workload Automation EE.

Encryption Between CA Workload Automation AE and CA Workload Automation EE

Data can be transferred between CA Workload Automation AE and CA Workload Automation EE with no encryption or with AES 128-bit encryption. Encryption occurs in two ways:

- The data received from CA Workload Automation EE
- The data sent to CA Workload Automation EE

The encryption settings on the scheduling managers must match.

Encryption of Data Received from CA Workload Automation EE

The encryption setting for CA Workload Automation AE is determined as follows:

- On UNIX—By the UseCommAliasEncryption parameter in the configuration file.
- On Windows—By the Use AES 128-bit encryption when communicating with zOS managers check box under the zOS Encryption tab on the Instance - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.

CA Workload Automation AE uses no encryption or AES 128-bit encryption to exchange data with CA Workload Automation EE. If you are using AES encryption, you must generate an instance-wide communication alias encryption file (cryptkey_alias.txt) in the $AUTOUSER.*instance_name* (on UNIX) or %AUTOUSER%.*instance_name* (on Windows) directory. The cryptkey_alias.txt file stores the communication alias encryption key. CA Workload Automation AE expects CA Workload Automation EE to encrypt the data using the key specified in the cryptkey_alias.txt file.

If you are using no encryption, CA Workload Automation AE expects the data it receives from CA Workload Automation EE to be unencrypted.

You must specify the same CA Workload Automation AE encryption setting in the CA Workload Automation EE AGENTDEF data set.

Important! You must set AES encryption only if AES encryption is also configured on CA Workload Automation EE. For more information about the encryption types that CA Workload Automation EE supports, see the CA Workload Automation EE documentation.

Note: If you do not know the key associated with the existing cryptkey_alias.txt file, you can regenerate the file using a new key. If CA Workload Automation AE works with other CA Workload Automation EE external instances, the administrator must update all AGENTDEF data sets with the new key.

Example: Using No Encryption When Receiving Data from CA Workload Automation EE

Suppose that you do not want the data received from CA Workload Automation EE to be encrypted. To use no encryption, you must set the UseCommAliasEncryption parameter to 0 in the configuration file (on UNIX) or clear the Use AES 128-bit encryption when communicating with zOS managers check box under the zOS Encryption tab on the Instance - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator (on Windows).

When you define your CA Workload Automation AE instance to CA Workload Automation EE, you must specify the NOENCRYPT operand, as follows:

```
COMMCHAN instancename_AGT ADDRESS(address) PORT(sched_aux_port) UNIX ASCII TCPIP
PREF(2) NOENCRYPT
```

Example: Using AES 128-Bit Encryption When Receiving Data from CA Workload Automation EE

Suppose that you want CA Workload Automation EE to encrypt data with AES 128-bit encryption. To use AES encryption, you must set the UseCommAliasEncryption parameter to 2 in the configuration file (on UNIX) or select the Use AES 128-bit encryption when communicating with zOS managers check box under the zOS Encryption tab on the Instance - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator (on Windows). After you set the communication alias encryption setting, you must generate the cryptkey_alias.txt file. When you generate the cryptkey_alias.txt file, you specify a key to secure and store in that file. On CA Workload Automation EE, you must issue the CRYPTKEY command using that same key. The CRYPTKEY command secures and stores the key using a key name on CA Workload Automation EE.

When you define your CA Workload Automation AE instance to CA Workload Automation EE, you must specify the key name using the ENCRYPT operand, as follows:

```
COMMCHAN ACE_AGT ADDRESS(address) PORT(sched_aux_port) UNIX ASCII TCPIP PREF(2)
ENCRYPT KEYNAME(keyname)
```

More information:

Configure the AGENTDEF Data Set on CA Workload Automation EE (see page 243)
Set Encryption for z/OS Communication on UNIX (see page 187)

Encryption of Data Sent to CA Workload Automation EE

The encryption setting for CA Workload Automation EE is determined by the MANAGER initialization parameter in the AGENTDEF data set. The following example shows the options:

```
MANAGER NAME(manager_name) {NOENCRYPT | ENCRYPT KEYNAME(keyname)}
```

If no encryption is specified, CA Workload Automation EE expects the data it receives from CA Workload Automation AE to be unencrypted.

If encryption is specified, CA Workload Automation EE expects CA Workload Automation AE to encrypt the data using the key name specified in the ENCRYPT operand.

On CA Workload Automation AE, you must specify the CA Workload Automation EE encryption setting using the xcrypt_type and xkey_to_manager attributes.

Example: Using No Encryption to Send Data to CA Workload Automation EE

Suppose that CA Workload Automation EE does not need the data transferred to be encrypted. To use no encryption, the NOENCRYPT operand is specified in the MANAGER initialization parameter of the AGENTDEF data set, as follows:

```
MANAGER NAME(manager_name) NOENCRYPT
```

When you define CA Workload Automation EE as an external instance to CA Workload Automation AE, you must specify the xcrypt_type: NONE attribute, as follows:

```
insert_xinst: external_instance_name
xtype: e
xmachine: host_name
xcrypt_type : NONE
xmanager: manager_name
xport: port_number
```

Example: Using AES 128-Bit Encryption to Send Data to CA Workload Automation EE

Suppose that CA Workload Automation EE needs the data transferred to be encrypted using AES 128-bit encryption. To use AES encryption, the ENCRYPT operand is specified in the MANAGER initialization parameter of the AGENTDEF data set, as follows:

```
MANAGER NAME(manager_name) ENCRYPT KEYNAME(keyname)
```

When you define CA Workload Automation EE as an external instance to CA Workload Automation AE, you must specify the xcrypt_type: AES and xkey_to_manager attributes, as follows:

```
insert_xinst: external_instance_name
xtype: e
xmachine: host_name
xcrypt_type: AES
xmanager: manager_name
xport: port_number
xkey_to_manager: key /* For AES encryption only */
```

Contact the CA Workload Automation EE administrator to get the key specified by ENCRYPT KEYNAME(*keyname*). You must enter the same key in the xkey_to_manager attribute. The *key* value must be prefixed with the hexadecimal identifier "0x" and must contain 32 characters. Valid characters are 0-9 and A-F, as shown in the following example:

```
key_to_manager: 0x0123456789ABCDEF0123456789ABCDEF
```

More information:

Define CA Workload Automation EE as an External Instance (see page 242)

How to Configure Dependencies with CA Workload Automation EE

You can create job dependencies between CA Workload Automation AE and CA Workload Automation EE. Before the scheduling managers can communicate with each other, you must configure them.

To configure dependencies with CA Workload Automation EE, follow these steps:

1. Configure the scheduler auxiliary listening port (see page 238).
2. Set encryption for z/OS communication (see page 187).
3. (AES 128-bit encryption only) Generate an instance-wide communication alias encryption file (see page 188).
4. Define CA Workload Automation EE as an external instance (see page 242).

5. Configure the AGENTDEF data set on CA Workload Automation EE (see page 243).
6. Verify the setup (see page 245).

After you set up this configuration, you can create job dependencies between the instances.

Configure the Scheduler Auxiliary Listening Port

The scheduler communicates with CA Workload Automation EE and CA WA Agent for z/OS using non-SSA ports. Therefore, you must disable port multiplexing and SSL encryption for the scheduler auxiliary listening port.

Note: If the port is already configured, skip this procedure.

To configure the scheduler auxiliary listening port

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Edit the following parameter in the configuration file as follows, and save the file:

   `SchedAuxiliaryListeningPort=`*`sch_port`*

   sch_port

   Defines the port number the scheduler uses to communicate with CA Workload Automation EE and the agent on z/OS. This port is used for all non-SSA communication.

   The scheduler auxiliary listening port is defined.
3. Enter the following commands at the operating system prompt:

   ```
   cd $CSAM_SOCKADAPTER/bin
   csamconfigedit Port=sch_port EnableSSL=False EnablePmux=False
   ```

   sch_port

   Specifies the port number to configure. You must specify the same scheduler auxiliary listening port that you specified in the SchedAuxiliaryListeningPort parameter in the configuration file.

   Port multiplexing and SSL encryption are disabled for the specified scheduler auxiliary listening port.
4. Enter the following command at the operating system prompt:

   ```
   unisrvcntr stop waae_sched.$AUTOSERV
   ```

   The scheduler stops.

5. Enter the following command at the operating system prompt:

   ```
   csampmux stop
   ```

   The csampmuxf process stops.

6. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start waae_sched.$AUTOSERV
   ```

   The scheduler starts. The scheduler auxiliary listening port is configured.

Note: For more information about the SchedAuxiliaryListeningPort parameter, see the *Administration Guide*.

Set Encryption for z/OS Communication on UNIX

CA Workload Automation AE uses no encryption or AES 128-bit encryption to exchange data with CA Workload Automation EE and CA WA Agent for z/OS. If you are using AES encryption, you must generate an instance-wide communication alias encryption file (cryptkey_alias.txt) in the $AUTOUSER.*instance_name* (on UNIX) or %AUTOUSER%.*instance_name* (on Windows) directory. The cryptkey_alias.txt file stores the communication alias encryption key.

Important! You must set AES encryption for z/OS communication only if AES encryption is also configured on CA Workload Automation EE or the agent on z/OS. For more information about the encryption types that CA Workload Automation EE and the agent on z/OS support, see the CA Workload Automation EE and CA WA Agent for z/OS documentation.

Notes:

- The current release of CA WA Agent for z/OS is r2.0. This release of the agent does not support AES 128-bit encryption. To run z/OS jobs using this agent, you must disable AES 128-bit encryption and use no encryption for z/OS communication. To disable AES encryption, you must set the UseCommAliasEncryption parameter to 0 in the configuration file.
- If CA Workload Automation AE works with other CA Workload Automation EE external instances or the agents on z/OS, the administrator must update all AGENTDEF data sets with the encryption setting.

To set encryption for z/OS communication on UNIX

1. Run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following commands at the operating system prompt:

   ```
   unisrvcntr stop waae_sched.$AUTOSERV
   unisrvcntr stop waae_server.$AUTOSERV
   ```

   The scheduler and the application server stop.

3. Edit the following parameter in the configuration file, and save the file:

   `UseCommAliasEncryption=0|2`

   0

   Specifies that no encryption is used.

   2

   Specifies that AES encryption is used to encrypt data.

   Note: If you set the UseCommAliasEncryption parameter to 2, you must generate the cryptkey_alias.txt file and specify the communication alias encryption key using the -a option of the as_config command.

4. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start waae_sched.$AUTOSERV
   unisrvcntr start waae_server.$AUTOSERV
   ```

   The scheduler and the application server start. The encryption for z/OS communication is set.

Notes:

- For information about specifying the encryption key using the as_config command, see the *Reference Guide*.
- On Windows, you can select the equivalent value using the Use AES 128-bit encryption when communicating with zOS managers check box under the zOS Encryption tab on the Instance - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator. For information about setting encryption for z/OS communication on Windows, see the *Online Help* or the *Windows Implementation Guide*.

Generate an Instance-Wide Communication Alias Encryption File

CA Workload Automation AE uses no encryption or AES 128-bit encryption to exchange data with CA Workload Automation EE and CA WA Agent for z/OS. If you are using AES encryption, you must generate the instance-wide communication alias encryption file (cryptkey_alias.txt).

The cryptkey_alias.txt file stores the communication alias encryption key. The cryptkey_alias.txt file is located in the $AUTOUSER.*instance_name* (on UNIX) or %AUTOUSER%.*instance_name* (on Windows) directory.

Important! Do this procedure only if AES encryption is also configured on CA Workload Automation EE or the agent on z/OS. For more information about the encryption types that CA Workload Automation EE and the agent on z/OS support, see the CA Workload Automation EE and CA WA Agent for z/OS documentation.

Notes:

- A CA Workload Automation AE instance can have only one cryptkey_alias.txt file. Before you do this procedure, check whether the file already exists. If the file exists, skip this procedure. You must provide the key associated with that file to the CA Workload Automation EE or agent administrator. They need the key to configure the AGENTDEF data set.
- If you do not know the key associated with the existing cryptkey_alias.txt, you can regenerate the file using a new key. If CA Workload Automation AE works with other CA Workload Automation EE external instances or the agents on z/OS, the administrator must update all AGENTDEF data sets with the new key.

To generate an instance-wide communication alias encryption file

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command at the operating system prompt:

   `as_config -a` *key*

   key

   Specifies the communication alias encryption key. You must prefix the hexadecimal identifier 0x to this value.

   Limits: Must contain 32 characters; valid characters are 0-9 and A-F.

   Note: This key must match the key stored in the ENCRYPT KEYNAME(*keyname*) parameter in the AGENTDEF data set of CA Workload Automation EE or the agent on z/OS.

   The communication alias encryption file (cryptkey_alias.txt) is generated with the encryption key. AES 128-bit encryption is used.

Define CA Workload Automation EE as an External Instance

Before you can create job dependencies between CA Workload Automation AE and CA Workload Automation EE, you must define CA Workload Automation EE as an external instance. All external instance entries are stored in the CA Workload Automation AE event server and can be reported using the autorep command.

To define CA Workload Automation EE as an external instance

1. Log on to the CA Workload Automation AE instance and do *one* of the following:
   - Issue JIL in interactive mode.
   - Open a JIL script in a text editor.
2. Specify the following definition:

   ```
   insert_xinst: external_instance_name
   xtype: e
   xmachine: host_name
   xcrypt_type : NONE | AES
   xmanager: manager_name
   xport: port_number
   ```

   Note: The xcrypt_type value must match the encryption setting specified in the MANAGER initialization parameter in the CA Workload Automation EE AGENTDEF data set.
3. If xcrypt_type is set to AES, specify the following additional attribute:

   ```
   xkey_to_manager: key
   ```

   key

   Specifies the encryption key defined on CA Workload Automation EE. This value must match the key specified by ENCRYPT KEYNAME(*keyname*) in the CA Workload Automation EE AGENTDEF data set. You must prefix the hexadecimal identifier 0x to this value.

   Limits: Must contain 32 characters; valid characters are 0-9 and A-F

   Example: 0x0123456789ABCDEF0123456789ABCDEF
4. Do *one* of the following:
   - Enter **exit** if you are using interactive mode.
   - Redirect the script to the jil command if you are using a script.

   The external instance is defined on CA Workload Automation AE.

Notes:

- Do this procedure for every CA Workload Automation EE instance that you want to create external job dependencies for.
- If you modify external instance entries while the CA Workload Automation AE scheduler is active, the scheduler handles the modifications in real time. You do not have to recycle the scheduler to create, update, and delete external instance entries.
- For more information about the insert_xinst JIL subcommand, see the *Reference Guide*.

More information:

Encryption of Data Sent to CA Workload Automation EE (see page 236)

Configure the AGENTDEF Data Set on CA Workload Automation EE

For communication to occur between CA Workload Automation AE and CA Workload Automation EE, you must configure the AGENTDEF data set on CA Workload Automation EE. The parameters in the AGENTDEF data set must match the settings defined on CA Workload Automation AE.

To configure the AGENTDEF data set, add the following entry:

```
COMMCHAN alias_name ADDRESS(sch_ip_address) PORT(sch_aux_port) platform +
ASCII TCPIP PREF(2) {NOENCRYPT|ENCRYPT KEYNAME(keyname)}
```

The following table describes the operands that are not self-explanatory and their corresponding CA Workload Automation AE settings:

AGENTDEF Operand	Description	Corresponding CA Workload Automation AE Setting
COMMCHAN *alias_name*	Specifies the name associated with the encryption data between CA Workload Automation AE and CA Workload Automation EE.	*INSTANCENAME*_AGT This is the communication alias for the CA Workload Automation AE scheduler. The value must be in uppercase. *INSTANCENAME* is the name of the CA Workload Automation AE instance.
ADDRESS(*sch_ip_address*)	Specifies the host name or the IP address of the computer where the CA Workload Automation AE scheduler is installed.	None

AGENTDEF Operand	Description	Corresponding CA Workload Automation AE Setting
PORT(*sch_aux_port*)	Specifies the port number that the CA Workload Automation AE scheduler uses for all non-SSA communication.	SchedAuxiliaryListeningPort parameter in the configuration file.
platform	Specifies whether the CA Workload Automation AE instance is installed on UNIX or Windows. Options are UNIX or NT.	None
NOENCRYPT | ENCRYPT KEYNAME(*keyname*)	Specifies the type of encryption used and the key that CA Workload Automation AE expects the data to be encrypted with. For AES encryption, you must secure and store the the key in a key name on CA Workload Automation EE. To generate the key name, use the CRYPTKEY command.	If NOENCRYPT is specified, xcrypt_type: NONE must be defined in the external instance definition, and the cryptkey_alias.txt file must not exist. If ENCRYPT KEYNAME(*keyname*) is specified, xcrypt_type: AES must be defined in the external instance definition. The same key must be stored in the cryptkey_alias.txt file in the $AUTOUSER.*instance_name* directory.

Note: For more information about the AGENTDEF data set on CA Workload Automation EE, see the *CA Workload Automation EE Installation and Configuration Guide*.

More information:

Encryption of Data Received from CA Workload Automation EE (see page 234)

Verify the Setup

After you configure cross-instance support on CA Workload Automation AE and CA Workload Automation EE, verify the configuration is set up properly.

To verify the setup

1. Enter the following command at the operating system prompt:

   ```
   autorep –X EE_external_instance [-q] [-n]
   ```

   -X *EE_external_instance*

   Specifies the external instance that you defined for CA Workload Automation EE.

   The autorep command is issued and a report is generated. If CA Workload Automation EE is successfully defined as an external instance, the report output is similar to the following:

   ```
   Name Type Server                          Port

   ____ ____ ______________________________ ____
   AES  e    server1                         16190
   ```

2. Enter the following command:

   ```
   autosyslog -e
   ```

   The scheduler log file is displayed. If the configuration is set up properly, the report output is similar to the following:

```
[10/21/2009 10:18:18]      CAUAJM_I_40245 EVENT: REFRESH_EXTINST
[10/21/2009 10:18:18]      CAUAJM_I_50407 Reading external instance information
[10/21/2009 10:18:18]      CAUAJM_I_50408 Instance=[AES]: Type=[e] Server=[server1] Port=[16190]
Manager Alias=[WAEEMGR]
```

Chapter 17: Configuring Cross-Instance Dependencies with CA UJMA and CA AutoSys WA Connect Option

This section contains the following topics:

CA UJMA and CA AutoSys WA Connect Option Dependencies

You can define jobs that have dependencies on jobs running on external machines (*external job dependencies*). These machines must be defined as *external instances* on CA Workload Automation AE. A CA Workload Automation AE job with these dependencies conditionally starts based on the status of the job running on the other instance. These dependencies are jobs that execute on an external instance but were not initiated on behalf of the local CA Workload Automation AE instance. When the dependent job completes, status information is sent to the local CA Workload Automation AE instance and recorded in the database. For example, a job in one instance can be defined to start based on the status of jobs running on a mainframe system.

Cross-Platform Scheduling Requirements

To work with CA UJMA and CA AutoSys WA Connect Option, the following components must be installed on the CA Workload Automation AE computer:

- CA Workload Automation AE scheduler (the component that communicates with CA AutoSys WA Connect Option and CA UJMA)
- CAICCI

Note: For more information about installing CAICCI, see the *CA Common Components Implementation Guide*.

You must have one of the following CA software products installed on the external machine that CA Workload Automation AE works with:

Software on the External Machine	Required Integration Software	Environment
CA UJMA	None	Distributed
CA Job Management Option	CA UJMA	Distributed
CA Jobtrac Job Management	CA UJMA or CA AutoSys WA Connect Option	Mainframe
CA Scheduler Job Management	CA UJMA or CA AutoSys WA Connect Option	Mainframe
CA Workload Automation EE	None	Mainframe
CA Workload Automation SE	CA UJMA or CA AutoSys WA Connect Option	Mainframe

Notes:

- CA UJMA requires TCP/IP.
- For more information about configuring cross-instance support on the external machine, see the documentation for the CA product installed on that machine.

CA UJMA

CA UJMA (CA Universal Job Management Agent) can run on distributed platforms as a standalone agent that executes binaries and scripts in a method similar to the agent for CA Workload Automation AE.

Additionally, all CA mainframe scheduling products can behave as CA UJMA agents, which lets the CA Workload Automation AE scheduler run jobs through those mainframe schedulers. In this scenario, the job being run is a named job known to the scheduler and is not a command or script.

Similarly, the CA Workload Automation AE scheduler can appear as a CA UJMA agent to other CA scheduler managers in the enterprise. In this scenario, the job submitted to the CA UJMA interface is a job defined to CA Workload Automation AE and is not a command or script.

You cannot create job dependencies on the mainframe using CA UJMA. To use mainframe job dependencies, you must install CA AutoSys WA Connect Option on the same computer as the mainframe scheduling manager

The scheduler uses CAICCI to communicate with CA UJMA agents.

Note: CA UJMA was formerly named Unicenter Universal Job Management Agent (UUJMA).

CA AutoSys WA Connect Option

CA AutoSys WA Connect Option (CA AutoSys Workload Automation Connect Option) lets the CA Workload Automation AE scheduler run jobs on mainframe scheduling managers. It also lets you create dependencies between jobs running on CA Workload Automation AE and the mainframe scheduling manager.

CA UJMA and CA AutoSys WA Connect Option Considerations

Consider the following points when you schedule jobs across platforms:

Maintaining cross-platform data in high availability mode:

If you are running CA Workload Automation AE in high availability mode, ensure the following so that job statuses and dependencies are not lost when the shadow scheduler takes over:

- The PRIMARYCCISYSID environment variable is correctly set on the primary and secondary schedulers and on the CA UJMA computers.
- Jobs and external dependencies were sent to the external instance with proper release levels to support PRIMARYCCISYSID.

Exit codes in CA Job Management Option:

When running a job from CA Job Management Option, you may need to modify the default fail codes currently set for the CA Job Management Option-defined job. Exit codes 2 through 99 are defined as the default fail codes for CA Job Management Option jobs. Therefore, an exit code of 0 to 1 indicates success. When you run a job from CA Job Management Option that executes a job in CA Workload Automation AE and the job fails with an exit code 1 (for example, bad command), the CA Workload Automation AE job ends with a status of FAILURE. However, the CA Job Management Option-defined job ends with a status of SUCCESS or COMPLETE. You must modify the fail codes to accommodate the differences in how success and failure are interpreted between the two scheduling managers. That is, you must define exit codes 1 through 99 as the fail codes for the CA Job Management Option-defined job and define only an exit code of 0 to indicate success.

Multiple CA Workload Automation AE instances running on one computer:

If more than one instance of CA Workload Automation AE runs on a single computer and you plan to activate the Cross-Platform Interface, only one instance of CA Workload Automation AE can run with the Cross-Platform Scheduling option set to a value of 2. Only one instance can function as an agent. That is, only one instance can accept job submissions from an external scheduling manager.

chase and autoping commands:

The chase and autoping commands return limited information about CA AutoSys WA Connect Option and CA UJMA jobs and computers.

Remote user authentication:

Remote user authentication is not supported for jobs running on CA AutoSys WA Connect Option. For CA UJMA jobs, remote user authentication is performed using the owner name associated with the job.

CHANGE_PRIORITY and SEND_SIGNAL events:

You cannot execute the CHANGE_PRIORITY and SEND_SIGNAL events on CA AutoSys WA Connect Option and CA UJMA jobs and computers.

CA UJMA and CA AutoSys WA Connect Option External Instance Types

To use external job dependencies, the scheduling manager or remote machine must be defined as an *external instance* in the CA Workload Automation AE database.

When you define CA UJMA or CA AutoSys WA Connect Option as an external instance, you must specify one of the following JIL attributes in the definition:

xtype: c

Indicates that CA AutoSys WA Connect Option is installed with the external scheduling manager. CA AutoSys WA Connect Option can be installed on the mainframe and supports cross-platform jobs and job dependencies. It lets you submit job requests to and receive job submissions from the following mainframe scheduling managers:

- CA Jobtrac Job Management
- CA Scheduler Job Management
- CA Workload Automation SE

The CA Workload Automation AE scheduler uses CAICCI to communicate with CA AutoSys WA Connect Option.

xtype: u

Indicates that CA UJMA is installed with the external scheduling manager or on the remote machine. CA UJMA can be installed on the mainframe, UNIX, and Windows. It lets you submit job requests to the remote machine where CA UJMA is installed. It lets you submit job requests to and receive job submissions from the following scheduling managers:

- CA Job Management Option
- CA Jobtrac Job Management
- CA Scheduler Job Management
- CA Workload Automation SE

The CA Workload Automation AE scheduler uses CAICCI to communicate with CA UJMA.

Note: Unlike CA AutoSys WA Connect Option, CA UJMA does not let you define cross-instance job dependencies on the mainframe. To define job dependencies on the mainframe, you must install CA AutoSys WA Connect Option on the same computer as the mainframe scheduling manager.

How to Configure Dependencies with CA UJMA and CA AutoSys WA Connect Option

You can create external job dependencies between CA Workload Automation AE and a machine running another CA scheduling manager. That external machine can run on a different platform, including mainframe.

Before you can create external job dependencies, you must configure CA Workload Automation AE.

To configure dependencies with CA UJMA and CA AutoSys WA Connect Option, follow these steps:

1. Ensure that the external machine that the dependent job runs on meets the requirements for cross-instance scheduling (see page 248).
2. Enable bi-directional scheduling on CA Workload Automation AE (see page 252).
3. Configure and start CAICCI (see page 253).
4. (High availability environments only) Configure failover support for cross-instance scheduling (see page 254).
5. Define the machine as an external instance on CA Workload Automation AE (see page 255).

After you set up this configuration, you can create job dependencies between CA Workload Automation AE and the external instance.

Enable Bi-Directional Scheduling on CA Workload Automation AE

To schedule jobs or create job dependencies on another CA scheduling manager, you must enable the CA Workload Automation AE instance to support bi-directional scheduling.

To enable bi-directional scheduling on CA Workload Automation AE

1. On the CA Workload Automation AE instance, log on as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command:

   ```
   sendevent -E STOP_DEMON
   ```

   The scheduler completes any processing it is currently performing and stops.

3. Edit the following parameter in the configuration file, and save the file:

   ```
   CrossPlatformScheduling=2
   ```

4. Enter the following command:

   ```
   eventor
   ```

   The scheduler starts.

5. Open the scheduler log (event_demon.$AUTOSERV) and check that it contains the following messages:

   ```
   CAUAJM_I_40005 Cross Platform Interface Initialization in progress
   CAUAJM_I_40015 Cross Platform Interface is now active
   ```

   The cross-platform scheduling interface is active and bi-directional (outbound and inbound) scheduling is enabled. The instance can send job requests to an agent and receive job requests from a scheduling manager.

Note: For more information about the CrossPlatformScheduling parameter and the configuration file ($AUTOUSER/config.$AUTOSERV), see the *Administration Guide*.

Configure and Start CAICCI

CAICCI is the communication layer that connects applications running on mainframe, UNIX, Windows, and other operating systems. You must configure and start CAICCI on CA Workload Automation AE before you can schedule jobs on the other systems.

To configure and start CAICCI

1. Log in as root on the CA Workload Automation AE instance.
2. Open the $CAIGLBL0000/cci/config/local_host/ccirmtd.prf file.
3. Edit the LOCAL and REMOTE parameters as follows, and save the file:

   ```
   LOCAL = local_host local_host 32768 startup
   REMOTE = remote_host cci_system_id 32768 startup port=7000
   ```

   CAICCI is configured.

4. Issue the following command:

   ```
   unicntrl start cci
   ```

   CAICCI restarts. The updated configuration settings are applied.

Configure Failover Support for Cross-Instance Scheduling

If you are using high availability mode, you can define the aliased CAICCI system ID on the local CA Workload Automation AE instance. The cross-platform interface of CA Workload Automation AE uses this CAICCI system ID to communicate with remote mainframe or UJMA nodes during failover. If the primary scheduler shuts down or becomes unreachable, all communication on the secondary scheduler proceeds as normal. Any statuses currently residing on the remote computers (mainframe or UJMA) are dispatched to the secondary scheduler computer for processing.

To configure failover support for cross-instance scheduling

1. Open the /etc/auto.profile file, edit the following variable, and save the file:

   `PRIMARYCCISYSID = cci_system_id`

   cci_system_id

   Defines the aliased CAICCI system ID specified in the ccirmtd configuration file.

   Note: This variable is initially configured during scheduler installation.

2. Restart the scheduler.

   Failover support is configured for cross-instance scheduling.

Define the Machine as an External Instance on CA Workload Automation AE

Before you can create external job dependencies, you must define the machine where the dependent job runs as an external instance on CA Workload Automation AE. All external instance entries are stored in the CA Workload Automation AE event server and can be reported using the autorep command.

To define the machine as an external instance on CA Workload Automation AE

1. Log on to the CA Workload Automation AE instance and do one of the following:
   - Issue JIL in interactive mode.
   - Open a JIL script in a text editor.
2. Specify the following definition:

   ```
   insert_xinst: external_instance_name
   xtype: c | u
   xmachine: host_name
   xcrypt_type : NONE | DEFAULT | AES
   xport: port_number
   ```

   xtype: c | u

   Specifies the external instance type. Options include the following:
   - c—Identifies a CA AutoSys WA Connect Option instance.
   - u—Identifies a CA UJMA or CA NSM instance.
3. If xcrypt_type is set to AES, specify the following additional attribute:

   ```
   xkey_to_manager: key
   ```
4. Repeat Steps 2 and 3 for each external instance that you want to communicate with.
5. Do *one* of the following:
   - Enter *exit* if you are using interactive mode.
   - Redirect the script to the jil command if you are using a script.

   The external instance is defined on CA Workload Automation AE.

Notes:

- If you modify external instance entries while the CA Workload Automation AE scheduler is active, the scheduler handles the modifications in real time. You do not have to recycle the scheduler to create, update, and delele external instance entries.
- For more information about the insert_xinst JIL subcommand, see the *Reference Guide*.

Example: Configure Cross-Instance Scheduling for CA Workload Automation SE

Suppose that you want to start jobs between a local CA Workload Automation AE instance and an external CA Workload Automation SE instance. You also want to create job dependencies between the instances, so CA AutoSys WA Connect Option is installed on the mainframe.

To configure cross-instance scheduling for CA Workload Automation SE:

1. Enable bi-directional scheduling on the local CA Workload Automation AE instance.
2. Configure and start CAICCI.
3. Define the CA Workload Automation SE machine on CA Workload Automation AE as follows, where remote3 is the CA Workload Automation SE host name:

   ```
   insert_machine: remote3
   type: c
   ```

   The type c indicates that CA Workload Automation AE uses CA AutoSys WA Connect Option installed on the mainframe to submit jobs to the mainframe and create cross-instance dependencies.

   Note: Alternatively, if you do not need to create cross-instance dependencies, you can submit jobs from CA Workload Automation AE directly to the mainframe. In this situation, you define the CA Workload Automation SE machine as follows:

   ```
   insert_machine: remote3
   type: u
   ```

4. Define a corresponding external instance for CA Workload Automation SE on CA Workload Automation AE as follows:

   ```
   insert_xinst: SE7
   xtype: c
   xmachine: remote3
   ```

5. Define the CA Workload Automation AE instance on CA Workload Automation SE.

After cross-platform scheduling is configured, you can define and submit jobs as follows:

- Suppose that you want to run a job named SE7JOBNM that is defined on CA Workload Automation SE. The job has no starting conditions and you want to submit it directly to CA Workload Automation SE. You can define the following Command job on CA Workload Automation AE:

  ```
  insert_job: SE_job1
  job_type: CMD
  command: SE7JOBNM
  machine: remote3 *
  date_conditions: 1
  days_of_week: all
  start_mins: 25
  ```

  Note: The machine definition for remote3 must have type **u**.

- Suppose that you want to run a job named SE7JOBNM that is defined on CA Workload Automation SE. The job has no starting conditions and you want to submit the job through CA AutoSys WA Connect Option, which is installed on CA Workload Automation SE. You can define the following Command job on CA Workload Automation AE:

  ```
  insert_job: SE_job2
  job_type: CMD
  command: auto_cnct -a remote3 -j SE7JOBNM -s CA7 -c RUN -d
  machine: remote3 *
  date_conditions: 1
  days_of_week: all
  start_mins: 25
  ```

  Note: The machine definition for remote3 must have type **c**, which indicates CA AutoSys WA Connect Option.

- Suppose that you want to submit two jobs with external dependencies. The first job depends on the JB5MINS job on the mainframe. The second job depends on the JB5HRS job on the mainframe. The jobs do not have starting conditions. You can define the following Command jobs on CA Workload Automation AE:

  ```
  insert_job: test_dep1
  job_type: CMD
  command: sleep 100
  condition: success(JB5MINS^RMT)
  machine: remote3

  insert_job: test_dep2
  job_type: CMD
  command: sleep 100
  condition: success(JB5HRS^RMT)
  machine: remote3
  ```

  Note: RMT is defined as an external instance on CA Workload Automation AE, and the machine definition for remote3 must have type **c**, which indicates CA AutoSys WA Connect Option. You can also define jobs as a combination of both Command jobs and external dependencies.

- Suppose that you want to run a job named ASYS7002 that is defined on CA Workload Automation SE. The job must run after the JB5HRS completes. The job has no starting conditions, and you want to submit it through CA AutoSys WA Connect Option, which is installed on CA Workload Automation SE. You can define the following Command job on CA Workload Automation AE:

  ```
  insert_job: SEjob4
  job_type: CMD
  command: auto_cnct -a remote3 -j ASYS7002 -s CA7 -c RUN -d
  machine: remote3
  condition: success(JB5HRS^RMT)
  ```

  Note: RMT is defined as an external instance on CA Workload Automation AE, and the machine definition for remote3 must have type **c**, which indicates CA AutoSys WA Connect Option.

Chapter 18: Configuring Cross-Platform Scheduling

This section contains the following topics:

Cross-Platform Scheduling

Cross-platform scheduling lets you schedule and reroute jobs between CA Workload Automation AE and other machines running on different platforms, including mainframe.

To use cross-platform scheduling, required components must be installed on the CA Workload Automation AE computer and on the external machine that CA Workload Automation AE works with. The scheduling manager or remote machine must also be defined as an *external instance* in the CA Workload Automation AE database.

More information:

Bi-Directional Scheduling

CA Workload Automation AE supports *bi-directional scheduling*, which lets you start jobs from remote machines (inbound) or submit jobs on remote machines (outbound).

With *inbound job scheduling*, CA Workload Automation AE acts as an agent and accepts job submissions from remote machines or other scheduling managers (such as CA Jobtrac Job Management and CA Workload Automation SE). The jobs are defined and run on the CA Workload Automation AE instance that is acting as an agent.

With *outbound job scheduling*, CA Workload Automation AE acts as a scheduling manager and sends job submissions to remote machines. The jobs are defined on the CA Workload Automation AE instance that is acting as a scheduling manager. The jobs run on the remote machine or other scheduling manager.

For example, a Linux Oracle instance can initiate jobs in a Windows Microsoft SQL Server instance, or a Windows Microsoft SQL Server instance can initiate jobs in a Solaris Oracle instance. You can add additional instances, such as Solaris Sybase, AIX Oracle, or HP Oracle instance, to the environment.

The CA Workload Automation AE cross-platform interface controls the bi-directional scheduling mode. You can configure the cross-platform interface to enable the following modes:

- Outbound job scheduling
- Inbound and outbound job scheduling (bi-directional scheduling)
- No cross-platform scheduling (the default)

Note: There are no restrictions on platforms, event servers, or number of instances when running in bi-directional scheduling mode.

How to Configure Cross-Platform Scheduling

From CA Workload Automation AE, you can submit jobs on a machine that is running on CA UJMA or another CA scheduling manager. That machine can run on a different platform, including mainframe. Similarly, CA Workload Automation AE can receive job submissions from the other machine.

Before you can submit jobs, you must configure cross-platform support.

Note: This process does not apply to CA Workload Automation EE. Bi-directional scheduling is currently not supported between CA Workload Automation AE and CA Workload Automation EE.

To configure cross-platform scheduling, follow these steps:

1. Ensure that the external machine that the job runs on meets the scheduling requirements (see page 248).
2. Enable bi-directional scheduling on CA Workload Automation AE (see page 252).
3. Configure and start CAICCI (see page 253).
4. (High availability environments only) Configure failover support for cross-platform scheduling (see page 254).
5. Define the external machine on CA Workload Automation AE (see page 263).
6. (CA UJMA only) Define CA UJMA user IDs and passwords on CA Workload Automation AE (see page 264).
7. Configure cross-platform support on the external machine, if needed.

   Note: For more information about configuring cross-platform support on the external machine, see the documentation for the CA product installed on that machine.

After you configure cross-platform scheduling, you can define and submit jobs between CA Workload Automation AE and the defined external machine.

Notes:

- To submit a job from CA Workload Automation AE to the mainframe, the job (specified in the command attribute in the job definition) must be defined as a valid job on the mainframe scheduling system.
- To submit a job from the mainframe to CA Workload Automation AE, the job (specified by the SUBFILE parameter of the mainframe job) must be defined as a valid job on CA Workload Automation AE.

Enable Bi-Directional Scheduling on CA Workload Automation AE

To schedule jobs or create job dependencies on another CA scheduling manager, you must enable the CA Workload Automation AE instance to support bi-directional scheduling.

To enable bi-directional scheduling on CA Workload Automation AE

1. On the CA Workload Automation AE instance, log on as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following command:

   ```
   sendevent -E STOP_DEMON
   ```

   The scheduler completes any processing it is currently performing and stops.
3. Edit the following parameter in the configuration file, and save the file:

   ```
   CrossPlatformScheduling=2
   ```
4. Enter the following command:

   ```
   eventor
   ```

   The scheduler starts.
5. Open the scheduler log (event_demon.$AUTOSERV) and check that it contains the following messages:

   ```
   CAUAJM_I_40005 Cross Platform Interface Initialization in progress
   CAUAJM_I_40015 Cross Platform Interface is now active
   ```

   The cross-platform scheduling interface is active and bi-directional (outbound and inbound) scheduling is enabled. The instance can send job requests to an agent and receive job requests from a scheduling manager.

Note: For more information about the CrossPlatformScheduling parameter and the configuration file ($AUTOUSER/config.$AUTOSERV), see the *Administration Guide*.

Configure and Start CAICCI

CAICCI is the communication layer that connects applications running on mainframe, UNIX, Windows, and other operating systems. You must configure and start CAICCI on CA Workload Automation AE before you can schedule jobs on the other systems.

To configure and start CAICCI

1. Log in as root on the CA Workload Automation AE instance.
2. Open the $CAIGLBL0000/cci/config/local_host/ccirmtd.prf file.
3. Edit the LOCAL and REMOTE parameters as follows, and save the file:

   ```
   LOCAL = local_host local_host 32768 startup
   REMOTE = remote_host cci_system_id 32768 startup port=7000
   ```

   CAICCI is configured.
4. Issue the following command:

   ```
   unicntrl start cci
   ```

   CAICCI restarts. The updated configuration settings are applied.

Configure Failover Support for Cross-Instance Scheduling

If you are using high availability mode, you can define the aliased CAICCI system ID on the local CA Workload Automation AE instance. The cross-platform interface of CA Workload Automation AE uses this CAICCI system ID to communicate with remote mainframe or UJMA nodes during failover. If the primary scheduler shuts down or becomes unreachable, all communication on the secondary scheduler proceeds as normal. Any statuses currently residing on the remote computers (mainframe or UJMA) are dispatched to the secondary scheduler computer for processing.

To configure failover support for cross-instance scheduling

1. Open the /etc/auto.profile file, edit the following variable, and save the file:

   ```
   PRIMARYCCISYSID = cci_system_id
   ```

   cci_system_id

   Defines the aliased CAICCI system ID specified in the ccirmtd configuration file.

   Note: This variable is initially configured during scheduler installation.
2. Restart the scheduler.

   Failover support is configured for cross-instance scheduling.

Define the External Machine on CA Workload Automation AE

Before you can submit jobs on an external machine running CA UJMA or another CA scheduling manager, you must define the machine on CA Workload Automation AE.

To define the external machine on CA Workload Automation AE

1. Log on to the CA Workload Automation AE instance and do one of the following:
   - Issue JIL in interactive mode.
   - Open a JIL script in a text editor.
2. Specify the following definition:

   ```
   insert_machine: host_name
   type: machine_type
   ```

   insert_machine: *host_name*

   Specifies the host name of the external machine.

   type: *machine_type*

   Specifies the type of machine you are defining. Options include the following:

   - c—Specifies a CA AutoSys WA Connect Option machine.
   - u—Specifies a CA UJMA or CA NSM machine.
3. Do *one* of the following:
   - Enter **exit** if you are using interactive mode.
   - Redirect the script to the jil command if you are using a script.

   The external machine is defined on CA Workload Automation AE.

Notes:

- Computers managed by CA UJMA cannot be part of a virtual machine. The job_load, max_load, and factor attributes are not supported for these types of computers.
- For more information about the insert_machine JIL subcommand, see the *Reference Guide*.

Define CA UJMA User IDs and Passwords on CA Workload Automation AE

After you define a CA UJMA machine to CA Workload Automation AE, you can define jobs to run on that machine. In a job definition, you can specify the CA UJMA machine using the machine definition. You specify the user ID that the job runs under using the owner attribute. The following example runs a job on the ZASYS400 computer under the user, bob:

```
insert_job: as400ji
owner: bob@ZASYS400
machine: ZASYS400
command: DLYJOB DLY(16)
```

The user specified in the owner attribute must have an account on the target CA UJMA computer. The account must match the owner value exactly for the job to run. You must specify the owner value as *user*@*machine*. Before you can specify a user in a job definition, you must define the user and its password on the local CA Workload Automation AE instance.

To define CA UJMA user IDs and passwords on CA Workload Automation AE

1. Log on to the CA Workload Automation AE instance as the EDIT superuser, and enter the following command:

   ```
   autosys_secure
   ```

   The following menu appears:

   ```
   Please select from the following options:
   [1] Activate EEM instance security.
   [2] Manage EDIT/EXEC superusers.
   [3] Change database password.
   [4] Change remote authentication method.
   [5] Manage user@host users.
   [6] Get Encrypted Password.
   [0] Exit CA WAAE Security Utility.
   ```

2. Enter 5 and press the Enter key.

   The following menu appears:

   ```
   Please select from the following options:
   [1] Create user@host or Domain password.
   [2] Change user@host or Domain password.
   [3] Delete user@host or Domain password.
   [4] Show all user@host users.
   [9] Exit from "Manage user@host users" menu.
   [0] Exit CA WAAE Security Utility.
   ```

3. Enter 1 and press the Enter key.
4. Enter the user name, user host or domain, and password information when prompted.

   Note: Where the operating system permits, CA UJMA user IDs can contain up to 30 alphanumeric characters. The user IDs can contain both uppercase and lowercase characters (when the operating system permits mixed case). You cannot use blank spaces and tab characters.

   The user is added. The following message appears:

   ```
   CAUAJM_I_60135 User Create successful.
   ```

5. Enter 0.

   You exit from the autosys_secure command. The data is loaded into the database.

Note: For more information about the autosys_secure command, see the *Reference Guide*.

Chapter 19: Configuring High Availability

This section contains the following topics:

Dual Event Servers

One of the ways that CA Workload Automation AE provides high availability is by running with two databases, or event servers. The other way is by using shadow and tie-breaker schedulers.

CA Workload Automation AE can run with two event servers. CA Workload Automation AE keeps these two event servers synchronized, which provides complete recovery when a failure occurs on one of the event servers. These two event servers contain identical data, including object definitions and events. CA Workload Automation AE reads from one event server and writes to both the event servers simultaneously.

When the scheduler processes events, it reads from both event servers. If it detects an event on one event server and not on the other, it copies the missing event to the other event server. Therefore, a temporary problem in getting events to one of the event servers does not interrupt processing.

Note: To avoid a single point of failure, the two event servers must reside on two different data servers running on different computers. For more information about event server rollover recovery, see the *Administration Guide*.

More information:

Shadow and Tie-Breaker Schedulers (see page 275)
Running Dual Event Server Mode (see page 26)

Considerations when Installing Dual Event Servers

You must install and configure the two databases before you can use them, and then set the appropriate configuration parameters.

When installing and configuring dual event servers, consider the following:

- The two event servers must reside on two different database servers, running on different computers, to avoid a single point of failure.
- The two event servers must have unique names.
- Both databases must be of the same type; for example Oracle.
- The scheduler does not start unless it can connect to both databases.

How to Install Dual Event Servers

To complete the installation of the dual event servers, follow these steps:

1. Install dual event servers (see page 268).

   Note: For Oracle or Sybase, install event servers on two different computers, specifying unique event server names.

2. Configure CA Workload Automation AE to run with dual event servers (see page 272).
3. Synchronize the two event servers (see page 273).

Install Dual Event Servers

You can install dual event servers on a computer that does not have CA Workload Automation AE installed on it. Dual event server mode ensures high availability of the database.

To install dual event servers

1. Install the event servers on two different database servers on two different computers, making sure the following is true:
   - The data server names are different.
   - The database sizes are the same.
2. Run the wa_setup.sh installation script.

   Note: For information about installing an event server, see the Installing the Server (see page 67) chapter in this guide.

   CA Workload Automation AE is installed.
3. Synchronize the databases.

More information:

Synchronizing Dual Event Servers (see page 273)

Install a Second Event Server

You can install a second event server in an environment where CA Workload Automation AE is running in single event server mode.

To install a second event server

1. Install the second event server on a different database server and a different computer, making sure that the following is true:
   - The data server name is different.
   - The database size is the same as your original database.
2. If you have not already done so, source the appropriate environment variables.
3. Load the database objects, as follows (instead of running the installation script):
   a. Change the directories to the following, as appropriate:
      - (Oracle) $AUTOSYS/dbobj/ORA
      - (Sybase) $AUTOSYS/dbobj/SYB
   b. Source the CA Workload Automation AE environment by running the following command:

      ```
      ./opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.shell.host
      ```

   c. Load the database objects into a new empty database, by issuing the following command, as appropriate:

      ```
      perl CreateAEDB.pl
      ```

      You are prompted for information to create the Oracle tablespaces or Sybase database.
4. Configure the database.
5. Synchronize the database.

More information:

Environment Variables (see page 41)
Configure CA Workload Automation AE to Run with Dual Event Servers (see page 272)
Synchronizing Dual Event Servers (see page 273)

autobcpDB Script—Synchronize Databases

The autobcp*DB* script synchronizes data servers on different computers to prepare them for dual event server mode. This script creates two identical servers based on the source data server.

Note: The autobcp*DB* script deletes all of the data in the target database and replaces it with the data in the source database. If you want to save the data in the target database, archive it before you run the autobcp*DB* script.

An autobcp*DB* script is included for each database vendor in the following directories:

- $AUTOSYS/dbobj/ORA/autobcpORA.pl (for Oracle)
- $AUTOSYS/dbobj/SYB/autobcpSYB.pl (for Sybase)

Notes:

- You must stop the scheduler and application server before you run the autobcp*DB* script.
- You can enter the autobcp*DB* script on a single line or in interactive mode which prompts you for the required information line by line.

This script has the following format:

For Oracle

```
perl autobcpORA.pl source_server target_server source_userid source_password
target_userid target_password dump_file oracle_directory
```

For Sybase

```
perl autobcpSYB.pl source_server source_db target_server target_db source_userid
source_password target_userid target_password dump_file
```

source_server

Defines the name of the source Oracle System ID (for example, AEDB) or Sybase server (for example, SourceServer). This is defined in the sql.ini file on Sybase and in the tnsnames.ora file on Oracle.

source_db

Defines the source Sybase database (for example, AEDB).

source_userid

Defines the user ID that is used to connect to the source Oracle System ID or Sybase server.

source_password

Defines the password that corresponds to the user ID that is used to connect to the source Oracle System ID or Sybase server.

target_server

Defines the target Oracle System ID (for example AEDB2) or Sybase server (for example, DestinationServer). This is defined in the sql.ini file on Sybase and in the tnsnames.ora file on Oracle.

target_db

Defines the target Sybase database (for example, AEDB2).

target_userid

Defines the user ID that is used to connect to the target Oracle System ID or Sybase server.

target_password

Defines the password that corresponds to the user ID that is used to connect to the target Oracle System ID or Sybase server.

dump_file

Defines the temporary file used in the transfer of data from one database to the other.

Default: dump.fil

oracle_directory

Defines the path to the Oracle directory.

Default: ORACLE_HOME

Example: Synchronize Databases on Sybase

This example copies data from the source database (AEDB) to the target database (AEDB2) on the source server (AUTOSYSDB) and the target server (AUTOSYSDB2).

Note: If you use the target user ID with the truncate command, the data is copied faster and reduces the database log requirements.

```
perl $AUTOSYS/dbobj/SYB/autobcpSYB.pl AUTOSYSDB AEDB AUTOSYSDB2 AEDB2 autosys
autosys sa autosys /tmp/dumpfile  | tee /tmp/autobcp.out
```

Configure CA Workload Automation AE to Run with Dual Event Servers

CA Workload Automation AE enables you to configure dual event servers.

To configure CA Workload Automation AE to run with dual event servers on Sybase

1. Modify the $AUTOUSER/config.$AUTOSERV configuration file using any text editor.

   In a single event server mode, there is only one event server listed in the configuration file. Following is a typical event server mode setting:

   ```
   # Specify the Databases
   #
   EventServer=aedb
   ```

   Modify the configuration file to add a line to define the second event server, similar to the following:

   ```
   EventServer=aedb
   EventServer=machine2::aedb
   ```

   Note: There must not be a comment character (#) at the beginning of the line that defines the second event server.

   The configuration file now points to two databases.

2. Define the appropriate database reconnect or rollover behavior in the $AUTOUSER/config.$AUTOSERV file. The DBEventReconnect parameter sets this behavior. The default setting is:

   ```
   # Number of times for Scheduler to attempt reconnect to Event Servers
   #
   DBEventReconnect=50
   #
   # USE the following for Dual Event Server Mode
   # DBEventReconnect=50,5
   ```

   By default, the reconnect or rollover behavior is set to single event server mode. For dual event server mode, use the DBEventReconnect parameter that consists of two values describing the connection and rollover behaviors.

   Place a comment character (#) at the beginning of the line used for single event server mode, for example:

   ```
   # DBEventReconnect=50
   ```

   Remove the comment character (#) from the beginning of the line used for dual event server mode, for example:

   ```
   DBEventReconnect=50,5
   ```

The default setting for dual event server mode specifies that the scheduler must attempt five connections with the event servers. If it cannot connect after five attempts, it must rollover to single event server mode, marking the other event server as *down*. Once in single event server mode, the scheduler must attempt a connection fifty times, and if it is unsuccessful, the scheduler shuts down.

Similarly, upon start up, the scheduler makes five attempts to connect to the event servers, and if unsuccessful, it immediately rolls over to a single event server mode, using the event server that is still functioning.

3. Save and exit the $AUTOUSER/config.$AUTOSERV file.
4. Ensure all server and client computers have connectivity to both event servers.

Synchronizing Dual Event Servers

The second event server must be synchronized with the first event server before you can begin processing using dual event server mode. This section describes this process.

The synchronization process is also used if CA Workload Automation AE has rolled over into single event server mode due to problems and you want to return to running with dual event servers.

Stop the Scheduler and Application Server

Before synchronizing the databases, you must stop all activity with the database. This can be accomplished by stopping the scheduler and all application servers.

To stop the scheduler and application servers

1. Issue the following command to stop the scheduler (you must be the EXEC superuser to do this):

   ```
   sendevent -E STOP_DEMON
   ```

   The scheduler stops. After the scheduler stops, no additional jobs are started.

2. Issue the following command (you must do this as root) to stop all application servers for the instance:

   ```
   unisrvcntr stop waae_server.$AUTOSERV
   ```

   The application server stops. This must be done on every computer that is running an application server. After all application servers for the instance have been stopped, no more editing happens with the database.

Start the Scheduler

Use the following command to bring up all the scheduler computers:

```
eventor
```

Each scheduler prints a message indicating that it is in dual event server mode.

The scheduler marks both event servers as being in dual event server mode. The application server checks the flags in both event servers for consistency. Therefore, you must start the scheduler before you start the application server. The application server cannot be started until after the scheduler has been started. This means that no thin client commands work. If you choose to run the autoping or chk_auto_up command before starting the scheduler, you must set the environment variable AS_TXLOCAL, which forces the client application to bypass the application server.

Important! This applies to all client applications running with that value set, so be sure to unset the variable before continuing.

Note: If CA Workload Automation AE is configured to run in dual event server mode, the scheduler does not start unless both the databases are available.

When you stop the scheduler, any jobs that are running, run to completion. You can run the autobcp*DB* script while the jobs are running on remote computers. In the worst-case scenario, there may be events on the source event server that are not stored on the target event server. This is not a problem, as the scheduler always reads from both event servers. If the scheduler finds an event on one server that is not on the other, it copies that event to the database that is missing it. If one event server missed an event due to recovery or network problems, this feature also dynamically synchronizes both event servers.

Note: While running the autobcpSYB.pl script on Sybase, ensure the following:

- Both event servers use the same ‘Character set’.
- The ‘LANG’ environment variable is unset from the shell or the command prompt window (from which the autobcpSYB.pl script is executed) using the following command:

  ```
  $ unset LANG
  ```

The autobcpSYB.pl script may have problems while copying data from one event server to another, and may fail with errors if the environment variables are different. For more information, see the Sybase documentation.

Start the Application Server

To start the application servers, run the following command (must be executed as root):

On Linux and Solaris, issue the following command:

```
/etc/init.d/waae_server.$AUTOSERV start
```

On AIX, issue the following command:

```
/etc/rc.d/waae_server.$AUTOSERV start
```

On HP-UX, issue the following command:

```
/sbin/init.d/waae_server.$AUTOSERV start
```

Now, the application servers run in dual event server mode and make updates to both the event servers.

Shadow and Tie-Breaker Schedulers

The scheduler interprets and processes the events it reads in the event server. It also schedules and starts jobs.

If you run CA Workload Automation AE with a shadow scheduler, the shadow scheduler takes over interpreting and processing events if the primary scheduler fails.

If you run CA Workload Automation AE with a shadow scheduler and dual event servers, a tie-breaker scheduler is required. It is a scheduler process that runs on a third node. It remains permanently idle and updates the event servers periodically to indicate its presence. The tie-breaker scheduler resolves contentions and eliminates situations in which one scheduler takes over because its own network is down.

Considerations when Installing Shadow and Tie-Breaker Schedulers

Consider the following when installing a shadow and tie-breaker scheduler:

- If running in high availability mode, you must have a primary and shadow scheduler.
- If running in high availability mode with dual event servers, you must have a primary, shadow, and tie-breaker scheduler.
- The scheduler computers must have application server and agents installed.
- The primary, shadow, and tie-breaker schedulers must all have the same instance name.
- The primary, shadow, and tie-breaker schedulers must use the same type of database.
- Ensure that the configuration parameters are identical for all schedulers, because the primary, shadow, and tie-breaker schedulers are typically installed on separate computers and with separate file systems for AUTOSYS and AUTOUSER.
- Install the software on a local drive on the primary, shadow, and tie-breaker scheduler computers, *not* on a network drive.

Install a Shadow Scheduler

One way that CA Workload Automation AE provides high availability is by running with a shadow scheduler. The shadow scheduler is designed to take over scheduling if the primary scheduler fails.

To install a shadow scheduler

1. Install the scheduler, application server, and an agent (an agent is installed automatically with a scheduler) on the computer where the shadow scheduler runs.

   Note: The primary, shadow, and tie-breaker schedulers can be installed on computers with different operating systems but must use the same type of database. All three schedulers must have the same instance name.

2. Edit the config.$AUTOSERV settings on the primary, shadow, and tie-breaker computers to specify the type of scheduler the computer will be.
3. Use the eventor command to start the scheduler service for the primary, shadow, and tie-breaker computers.
4. Enter autosyslog -e at a CA Workload Automation AE operating system prompt.

   You can view the startup progress.

Note: When you stop the primary scheduler with the sendevent -E STOP_DEMON command, the shadow and tie-breaker schedulers continue to run.

Install a Tie-Breaker Scheduler

If you run CA Workload Automation AE with a shadow scheduler and dual event servers, a Tie-breaker scheduler is required. It is a scheduler process that runs on a third node. It remains permanently idle and updates the event servers periodically to indicate its presence. The tie-breaker scheduler resolves contentions and eliminates situations in which one scheduler takes over because its own network is down.

To install a tie-breaker scheduler

1. Install the scheduler, application server and an agent (an agent is installed automatically with a scheduler) on the computer where the tie-breaker scheduler runs.

   Note: The primary, shadow, and tie-breaker schedulers can be installed on computers with different operating systems but must use the same type of database. All three schedulers must have the same instance name.

2. Edit the config.$AUTOSERV settings on the primary, shadow, and tie-breaker computers to specify the type of scheduler the computer will be.

3. Use the eventor command to start the scheduler service for the primary, shadow, and tie-breaker computers.

4. Enter autosyslog -e at a CA Workload Automation AE operating system prompt.

   You can view the startup progress.

Note: When you stop the primary scheduler with the sendevent -E STOP_DEMON command, the shadow and tie-breaker schedulers continue to run.

Restore the Primary Scheduler

If you run CA Workload Automation AE with a shadow scheduler, the shadow scheduler takes over interpreting and processing events if the primary scheduler fails. You can restore the primary scheduler after the shadow scheduler takes over.

To restore the primary scheduler

1. Enter the following command at the operating system prompt:

   ```
   sendevent –E STOP_DEMON
   ```

   The shadow stops. You can restart the primary and shadow schedulers.

2. Enter the following command at the operating system prompt:

   ```
   eventor
   ```

   The primary scheduler is restored.

Note: Even though the primary scheduler is restored, CA Workload Automation AE does not switch to high availability mode. You must stop the shadow scheduler and start the primary scheduler to run CA Workload Automation AE in high availability mode.

More information:

Start the Scheduler (see page 90)

How High Availability Is Configured

When you configure CA Workload Automation AE in high availability mode, you must stop and start the agent, scheduler, and application server. The scheduler must be started manually on the primary and the shadow scheduler.

In the config.$AUTOSERV file, you must set the following parameters when configuring CA Workload Automation AE in high availability mode:

RoleDesignator

Specifies whether the scheduler is a primary, shadow, or tie-breaker scheduler.

HAPollInterval

Checks if any schedulers have gone down in the seconds specified.

AutoServer

Tells the agents to return events to the correct application server. This parameter is used when a rollover occurs from primary to shadow scheduler.

EventServer

Defines the logical name of the CA Workload Automation AE database.

The following process describes how to configure CA Workload Automation AE in high availability mode, where computer1 is a primary scheduler and event server A, and computer2 is a shadow scheduler:

1. Stop the scheduler and application server on computer1.
2. Stop the scheduler and application server on computer2.
3. Set the following in config.$AUTOSERV file on computer1:
   a. RoleDesignator to 1 (Primary)
   b. HAPollInterval=5
   c. AutoServer=machine1,machine2
4. Set the following in config.$AUTOSERV file on computer2:
   a. RoleDesignator to 2 (Shadow)
   b. HAPollInterval=5
   c. EventServer=machine1::AEDB
   d. AutoServer=machine2,machine1
5. Start the scheduler and application server on computer1.
6. Start the scheduler and application server on computer2.
7. Run autosyslog –e command on computer 1. The following output is displayed:

```
-
[08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in single server
mode.  Event server 1:  AEDB.
[08/08/2005 10:46:17]      CAUAJM_I_50407 Reading external instance
information
[08/08/2005 10:46:17]      CAUAJM_I_50408 No external instance information
available.
[08/08/2005 10:46:17]      CAUAJM_I_40319 CA Workload Automation AE Primary
Scheduler active.
[08/08/2005 10:46:27]      CAUAJM_I_00151 The system is running in High-
availability mode.
-
```

8. Run autosyslog –e command on computer 2. The following output is displayed:

```
-
[08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in single server
mode.  Event server 1:  machine1::AEDB.
[08/08/2005 10:46:17]      CAUAJM_I_50407 Reading external instance
information
[08/08/2005 10:46:17]      CAUAJM_I_50408 No external instance information
available.
[08/08/2005 10:46:17]      CAUAJM_I_40319 CA Workload Automation AE Shadow
Scheduler active.
[08/08/2005 10:46:27]      CAUAJM_I_00151 The system is running in High-
availability mode.
-
```

   Note: Now you are in high availability mode. If you make changes to the configuration, you need to stop the scheduler and application server.

9. Stop the scheduler and application server on computer2.

10. Run the autosyslog –e command on computer 1. The following output is displayed:

```
-
[08/08/2005 10:44:42]      CAUAJM_I_00152 The Shadow has been shutdown.  The
system is no longer in High-availability mode.
-
```

    You can stop the shadow scheduler and the primary scheduler acknowledges this. You can now start the shadow scheduler and CA Workload Automation AE returns to high availability mode.

More information:

Stop the Scheduler and Application Server (see page 273)
Start the Scheduler (see page 90)
Start the Application Server (see page 91)

How High Availability with Dual Event Servers Is Configured

When CA Workload Automation AE runs in high availability mode with dual event servers, you must have a tie-breaker scheduler that is used, if both a scheduler and an event server go down. The scheduler must be started manually on each computer.

In the config.$AUTOSERV file, you must set the following parameters when configuring CA Workload Automation AE in high availability mode with dual event servers:

RoleDesignator

Specifies whether the scheduler is a primary, shadow, or tie-breaker scheduler.

HAPollInterval

Checks if any schedulers have gone down in the seconds specified.

AutoServer

Tells the agents to return events to the correct application server. This parameter is used when a rollover occurs from primary to shadow scheduler.

EventServer

Defines the logical name of the CA Workload Automation AE database.

The following process describes how to configure CA Workload Automation AE in high availability mode with dual event servers, where computer1 is a primary scheduler and event server A, computer2 is a shadow scheduler and event server B, and computer3 is a tie-breaker scheduler:

1. Stop the scheduler and application server on computer1.
2. Stop the scheduler and application server on computer2.
3. Stop the scheduler and application server on computer3.

4. Set the following in config.$AUTOSERV file on computer1:
    a. RoleDesignator to 1 (Primary)
    b. HAPollInterval=5
    c. DBEventReconnect=50,5
    d. EventServer=AEDB
    e. AutoServer=machine1,machine2,machine3
    f. EventServer=machine2::AEDB
5. Set the following in config.$AUTOSERV file on computer2:
    a. RoleDesignator to 2 (Shadow)
    b. HAPollInterval=5
    c. DBEventReconnect=50,5
    d. EventServer=AEDB
    e. AutoServer=machine2,machine1,machine3
    f. EventServer=machine1::AEDB
6. Set the following in config.$AUTOSERV file on computer3:
    a. RoleDesignator to 3 (Tie-breaker)
    b. HAPollInterval=5
    c. DBEventReconnect=50,5
    d. AutoServer=machine3,machine1.machine2
    e. EventServer=machine1::AEDB
    f. EventServer=machine2::AEDB
7. Start the scheduler and application server on computer1.
8. Start the scheduler and application server on computer2.
9. Start the scheduler and application server on computer3.

10. Run autosyslog –e command on computer 1. The following output is displayed:

```
-
[08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in dual event
server mode.  Event server 1:  AEDB.  Event server 2:  machine2::AEDB.
[08/08/2005 10:46:17]      CAUAJM_I_50407 Reading external instance
information
[08/08/2005 10:46:17]      CAUAJM_I_50408 No external instance information
available.
[08/08/2005 10:46:17]      CAUAJM_I_40319 CA Workload Automation AE Primary
Scheduler active.
[08/08/2005 10:46:27]      CAUAJM_I_00151 The system is running in High-
availability mode.
-
```

11. Run autosyslog –e command on computer 2. The following output is displayed:

```
-
[08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in dual event
server mode.  Event server 1:  machine1::AEDB.  Event server 2:  AEDB.
[08/08/2005 10:46:17]      CAUAJM_I_50407 Reading external instance
information
[08/08/2005 10:46:17]      CAUAJM_I_50408 No external instance information
available.
[08/08/2005 10:46:17]      CAUAJM_I_40319 CA Workload Automation AE Shadow
Scheduler active.
[08/08/2005 10:46:27]      CAUAJM_I_00151 The system is running in High-
availability mode.
-
```

12. Run autosyslog –e command on computer 3. The following output is displayed:

```
-
[08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in dual event
server mode.  Event server 1:  machine1::AEDB.  Event server 2:
machine2::AEDB.
[08/08/2005 10:46:17]      CAUAJM_I_50407 Reading external instance
information
[08/08/2005 10:46:17]      CAUAJM_I_50408 No external instance information
available.
[08/08/2005 10:46:17]      CAUAJM_I_40319 CA Workload Automation AE Tie-
breaker Scheduler active.
[08/08/2005 10:46:27]      CAUAJM_I_00151 The system is running in High-
availability mode.
-
```

Note: Now you are in high availability mode with dual event servers. If you make changes to the configuration, you must stop the scheduler and application server.

13. Stop the scheduler and application server on computer2.

14. Run the autosyslog –e command on computer1. The following output is displayed:

```
-
```

```
[08/08/2005 10:44:42]      CAUAJM_I_00152 The Shadow has been shutdown.  The
system is no longer in High-availability mode.
-
```

You can stop the shadow or tie-breaker scheduler and the primary scheduler acknowledges this. You can now start the shadow or tie-breaker scheduler and CA Workload Automation AE returns to high availability mode.

Chapter 20: Configuring CA Workload Automation AE with Red Hat Cluster Manager

CA Workload Automation AE can cooperate with Red Hat Cluster Suite to form a highly-available CA Workload Automation AE scheduler and application server. In this configuration, Red Hat Cluster Manager replaces the built-in high availability features of CA Workload Automation AE. The Cluster Manager selects a node on which to run each CA Workload Automation AE service. CA Workload Automation AE clients refer to a floating IP address, which the Cluster Manager assigns to the node running the CA Workload Automation AE application server.

A highly-available CA Workload Automation AE scheduler and application server require a highly-available database. The procedures for preparing a highly-available database vary depending on the type of database used. For information about using other databases, refer to the documentation for those databases.

Note: For more information about configuring and managing the Cluster Manager, see the Red Hat Cluster Suite documentation.

This section contains the following topics:

Installation Considerations

Select an additional host name and IP address for the clustered CA Workload Automation AE application server. Define this name and address in your DNS or other name service. The examples in this section use the addresses and names in the following table:

IP Address	Host Name	Description
192.168.34.3	arsis	first node in the cluster
192.168.34.4	thesis	second node in the cluster
192.168.34.5	iambus	floating AppServer address

Install the CA Workload Automation AE components you want on each computer in the cluster. Install the scheduler and application server on multiple computers, if you want the Red Hat Cluster Manager to control them.

Server Installation

Make the following selections during CA Workload Automation AE installation, on the computers you intend to run the scheduler, application server, or both:

- In the Application Server Properties dialog, clear the Set the application server to start automatically at system startup time and Start the application server following installation check boxes. The Cluster Manager controls the application server.
- In the Scheduler Properties dialog, clear the Set the scheduler to start automatically at system startup time and Start the scheduler following installation check boxes. Also, do not select the Configure High Availability check box. The Cluster Manager controls the scheduler.
- After installation, edit the $AUTOUSER/config.$AUTOSERV file. Change the AutoServer value from the local host name to the floating host name you selected for the application server. For example, the config.ACE file on both arsis and thesis contains:

  ```
  AutoServer=iambus
  ```

Client Installation

When installing CA Workload Automation AE clients in the cluster or elsewhere on the network, use the floating host name you selected for the application server. For example, iambus.

Configuring Cluster Services

Use the Red Hat Cluster Management application to create the CA Workload Automation AE services in your cluster configuration.

For the CA Workload Automation AE application server service, do the following:

- Define a script resource with file /etc/init.d/waae_server.ACE, substituting your CA Workload Automation AE instance name, if it differs from the default ACE.
- Attach an IP address resource to the script resource, which contains the floating IP address you defined for the application server, that is, 192.168.34.5.

For the CA Workload Automation AE scheduler service, define a script resource with file /etc/init.d/waae_sched.ACE, substituting your CA Workload Automation AE instance name, if it differs from the default ACE.

Create a Failover Domain for each set of nodes on which you intend to run the CA Workload Automation AE services. Set the appropriate Failover Domain in each service. If you have installed both CA Workload Automation AE components on the same set of nodes, they can share the same Failover Domain.

Managing Cluster Services

Use the Red Hat Cluster Management application or command line tools to start and stop the cluster services. Avoid using a STOP_DEMON event to stop the scheduler. The Cluster Manager considers the scheduler service to have failed and restarts it.

The following example displays the status of a cluster as reported by the clustat command:

```
$ clustat
Member Status: Quorate, Group Member
Member Name                              State      ID
------ ----                              -----      --
arsis                                    Online     0x0000000000000001
thesis                                   Online     0x0000000000000002
Service Name         Owner (Last)                   State
------- ----         ----- ------                   -----
WAAE AppServer       thesis                         started
WAAE Scheduler       arsis                          started
```

Defining Jobs

You can define CA Workload Automation AE jobs to run on specific computers in the cluster, or on a computer that is currently assigned a particular IP address resource.

The following example displays a simple set of jobs:

```
insert_machine: arsis
type: r
insert_machine: thesis
type: r
insert_machine: iambus
type: r
insert_job: arsis_id
machine: arsis
command: sendevent -E SET_GLOBAL -g arsis_is=`uname -n`
insert_job: server_id
machine: iambus
command: sendevent -E SET_GLOBAL -g server_is=`uname -n`
insert_job: thesis_id
machine: thesis
command: sendevent -E SET_GLOBAL -g thesis_is=`uname -n`
```

Each job records the name of the node on which it runs in a global variable. The following results are displayed after sending a STARTJOB event for each job:

```
$ autorep -G %_is
Global Name                Value                      Last Changed
-------------------------  -------------------------  -------------------
arsis_is                   arsis                      11/14/2009 14:32:57
server_is                  thesis                     11/14/2009 14:33:26
thesis_is                  thesis                     11/14/2009 14:33:03
```

The Cluster Manager assigned the CA Workload Automation AE AppServer's IP address resource, iambus, to thesis at the time the jobs ran. The jil, sendevent, and autorep commands and the CA Workload Automation AE agents also used that address to communicate with the application server.

Chapter 21: Configuring CA Workload Automation AE to Work with Other CA Products

This section contains the following topics:

CA Service Desk Integration

You can integrate CA Workload Automation AE with CA Service Desk to let you open a service desk ticket (request or incident) when a job fails.

CA Service Desk is an enterprise-level service desk solution that lets you automate IT processes and provide audit trails for regulatory compliance. CA Service Desk is installed as a standalone product. CA Service Desk provides a self-service web interface that helps customers resolve their own issues. From this web interface, they can submit tickets, check status, and browse the knowledge base. To initiate a service desk ticket to CA Service Desk, CA Workload Automation AE requires the web service desk URL, login identifier, and password. If you use a web service customer to access CA Service Desk, the web service desk customer can be substituted for the web service desk login identifier and password.

The default data files that are added to the CA Service Desk database during configuration are used to create requests through the web services. In addition to the data files, CA Service Desk provides the default templates and contacts for CA Workload Automation AE. That is, the default users and templates use the names of CA Workload Automation AE.

Note: Only the CA Service Desk administrator is authorized to modify the default templates that are provided during the configuration process.

How to Integrate CA Workload Automation AE with CA Service Desk

This topic provides an overview of the steps that you must perform to integrate CA Workload Automation AE with CA Service Desk.

To integrate CA Workload Automation AE with CA Service Desk, follow these steps:

1. Configure CA Workload Automation AE to work with CA Service Desk (see page 290).
2. Initiate a Service Desk ticket using CA Workload Automation AE (see page 292).

Configure CA Workload Automation AE to Work with CA Service Desk

CA Workload Automation AE works with CA Service Desk to let you open a service desk ticket (request or incident) when a job fails. To integrate CA Workload Automation AE with CA Service Desk, you must issue an integration command on CA Service Desk and activate the Service Desk interface on CA Workload Automation AE.

The ServiceDeskCust, ServiceDeskURL, and ServiceDeskUser parameters let you activate the Service Desk interface. You must set either the ServiceDeskURL and ServiceDeskUser parameters, or the ServiceDeskURL and ServiceDeskCust parameters to activate the Service Desk interface. When you set these service desk parameters, the scheduler initiates the opening of a service desk ticket through CA Service Desk if the job the scheduler is processing was defined with the appropriate service desk attributes.

Notes:

- CA Workload Automation AE requires CA Service Desk r11 or r11.2.
- By default, CA Service Desk integration is inactive.

To configure CA Workload Automation AE to work with CA Service Desk

1. Open the CA Service Desk application and verify that it operates properly.
2. Access the following location:

   ```
   C:\Program Files\CA\Service Desk\data\integrations
   ```

3. Run *one* of the following commands:

   ```
   pdm_load –f itil_integAutoSys.dat
   ```

   Specifies an ITIL configured CA Service Desk installation.

   ```
   pdm_load –f integAutoSys.dat
   ```

   Specifies a default or non-ITIL configured CA Service Desk installation.

4. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
5. Enter the following command at the operating system prompt:

   ```
   unisrvcntr stop waae_sched.$AUTOSERV
   ```

   The scheduler completes any processing it is currently performing and stops.
6. Edit the following parameters in the configuration file, and save the file:

   ```
   ServiceDeskURL=web_server_site
   ```

   web_server_site

   Defines the address for the CA Service Desk web service.

   Example: http://servicedeskhost:8080/axis/services/USD_R11_WebService

   ```
   ServiceDeskUser=user/password
   ```

   user/password

   Defines the user name and its associated password that is used to connect to the CA Service Desk web service.

   ```
   ServiceDeskCust=web_server_customer
   ```

   web_server_customer

   Defines the customer name for the CA Service Desk web service.

   Note: The ServiceDeskCust parameter can be substituted for the ServiceDeskUser parameter. That is, if you use a web service customer to access CA Service Desk, you can update the ServiceDeskCust parameter instead of the ServiceDeskUser parameter.

   Note: On Windows, you can enter the equivalent value using the URL Location, Web Service Login ID, Web Service Login Password, and Web Service Customer fields in the Service Desk pane on the Integration - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator. For more information about configuring CA Workload Automation AE to work with CA Service Desk on Windows, see the *Online Help*.
7. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start waae_sched.$AUTOSERV
   ```

   The scheduler starts. CA Workload Automation AE is configured to work with CA Service Desk, and you can now open a service desk ticket.

Initiate a Service Desk Ticket Using CA Workload Automation AE

The integration of CA Service Desk and CA Workload Automation AE lets you open a service desk ticket (request or incident) when a job fails. When a job is defined to open a service desk ticket, the CA Workload Automation AE scheduler initiates the opening of the ticket during terminal status processing. The scheduler prepares and sends the ticket. Messages are written to the scheduler log indicating whether the ticket was sent and processed successfully.

To initiate a service desk ticket using CA Workload Automation AE, specify the following attributes in the job definition:

- service_desk
- (Optional) svcdesk_desc
- (Optional) svcdesk_pri
- (Optional) svcdesk_imp
- (Optional) svcdesk_sev
- (Optional) svcdesk_attr

Notes:

- Only the service_desk attribute is required. If the optional attributes are not set, the job uses the CA Workload Automation AE service desk template values set in CA Service Desk. This template is included in the CA Service Desk installation. Before initiating a service desk ticket, make sure that the web services for CA Service Desk are active.
- For more information about the service desk attributes of a job, see the *Reference Guide* and the *User Guide*.

Example: Initiate a Service Desk Incident

This example initiates a service desk incident with a priority of 1 for a job named service_desk_on_failure_1.

```
insert_job: service_desk_on_failure_1
machine: localhost
command: false
owner: user@localhost
service_desk: y
svcdesk_pri: 1
svcdesk_desc: “service_desk_on_failure_1 has failed.”
```

Example: Initiate a Service Desk Request

This example initiates a service desk request with an impact of 3 and a severity of 4 for a job named service_desk_on_failure_2.

```
insert_job: service_desk_on_failure_2
machine: localhost
command: false
owner: user@localhost
service_desk: y
svcdesk_imp: 3
svcdesk_sev: 4
svcdesk_desc: “service_desk_on_failure_2 has failed.”
```

CA Spectrum Automation Manager Integration

You can integrate CA Workload Automation AE with CA Spectrum Automation Manager for load balancing and scheduling based on real-time resource usage.

With CA Spectrum Automation Manager, you can do the following:

- Select the best machine for CA Workload Automation AE to run a job.
- Schedule work based on the availability of real-time resources (for example, CPU usage, memory, operating system, and installed software components).

To enable best machine selection, you must create CA Workload Automation AE machine pools that are similar in definition to the existing CA Workload Automation AE virtual machines. A machine pool contains a list of CA Workload Automation AE real machines that are monitored by CA Spectrum Automation Manager. When a job is defined to reference a machine pool name or real resource dependencies, CA Spectrum Automation Manager is used for machine selection.

You can use real resource monitoring with machine pools.

Note: For more information about real resource monitoring, see the *User Guide*.

Installation Considerations

The following are important considerations when you install CA Spectrum Automation Manager:

- CA Spectrum Automation Manager and CA Application Configuration Manager (CA ACM) are not shipped with CA Workload Automation AE.
- The CA Spectrum Automation Manager must be installed on a machine accessible through web services to the CA Workload Automation AE schedulers and application servers. You must install CA ACM if you want to monitor software metrics. For more information about integrating CA ACM to work with CA Workload Automation AE, see the CA Spectrum Automation Manager documentation.
- The CA Spectrum Automation Manager agents (CA SysEdge and CA ACM agents) must be installed on all agent machines that utilize real resources for load balancing. The SysEdge agents monitor all real resource metrics except for the software and CPU speed metrics. The software and CPU speed metrics are monitored by CA ACM agents.

  Notes:

  - If SysEdge is not running, the agent machine is not qualified for job submission although it satisfies the real resource constraints.
  - You must install the CA ACM agents only if you want to monitor the software and CPU speed metrics.
  - CA Workload Automation AE supports only some of the metrics that the SysEdge agents monitor. To enable the SysEdge agents to monitor the real resource metrics, you must discover the SysEdge agents and enable them using the Discovery tool provided by CA Spectrum Automation Manager. For information about the real resource metrics that CA Workload Automation AE supports, see the *User Guide*. For information about enabling SysEdge and CA ACM agents and discovering machines, see the CA Spectrum Automation Manager documentation.
- To use real resource dependencies, the CA Spectrum Automation Manager SDK client must be installed on the CA Workload Automation AE scheduler and application server machines and the SDK library must be included in the SYSTEM path.

  Note: If you are running CA Workload Automation AE in high availability mode, you must ensure that the CA Spectrum Automation Manager SDK clients are installed on all CA Workload Automation AE servers running in high availability mode for CA Workload Automation AE to communicate successfully with CA Spectrum Automation Manager.

Configure CA Workload Automation AE to Work with CA Spectrum Automation Manager

CA Workload Automation AE works with CA Spectrum Automation Manager for load balancing and scheduling based on real-time resource usage. To integrate CA Workload Automation AE with CA Spectrum Automation Manager, you must install the CA Spectrum Automation Manager SDK client on the CA Workload Automation AE server. The CA Spectrum Automation Manager SDK client is required for communication between CA Workload Automation AE and CA Spectrum Automation Manager.

When you set the DCAURL and DCAUser parameters, CA Workload Automation AE integrates with CA Spectrum Automation Manager to monitor machines.

Note: By default, CA Spectrum Automation Manager integration is inactive.

To configure CA Workload Automation AE to work with CA Spectrum Automation Manager

1. Log on to CA Workload Automation AE as the EXEC superuser and run the shell that is sourced to use CA Workload Automation AE.
2. Enter the following commands at the operating system prompt:

   ```
   unisrvcntr stop waae_sched.$AUTOSERV
   unisrvcntr stop waae_server.$AUTOSERV
   ```

   The scheduler and the application server stop.
3. Edit the following parameters in the configuration file, and save the file:

   DCAURL=*web_server_site*

   web_server_site

   Defines the address for the CA Spectrum Automation Manager web service.

   Example: https://dcamanager:443/dpm/sc

   Note: You can also access CA Spectrum Automation Manager using https://dcahostname:8443/UI/DPMUI.html.

   DCAUser=*WebSvcId**EncryptedPassword*

   WebSvcId**EncryptedPassword

   Defines the user name and its associated password that is used to connect to the CA Spectrum Automation Manager web service.

   Note: The password is encrypted and defined using the autosys_secure command.

4. Add the Spectrum Automation Manager SDK library path at the end of the aslibs environment variable in the shell script that contains the environment variables you want to source.

   The aslibs environment variable is modified to include the directory where the SDK libraries reside.

5. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start waae_sched.$AUTOSERV
   ```

   The scheduler starts and writes Spectrum Automation Manager specific information to the CA Workload Automation AE database.

6. Enter the following command at the operating system prompt:

   ```
   unisrvcntr start waae_server.$AUTOSERV
   ```

   The application server starts. It reads the information from the CA Workload Automation AE database and connects to Spectrum Automation Manager. CA Workload Automation AE is configured to work with CA Spectrum Automation Manager, and you can now schedule jobs or provision CA Workload Automation AE agents using CA Spectrum Automation Manager.

Note: On Windows, you can enter the equivalent values using the URL Location, Web Service Login ID, and Web Service Login Password fields in the Spectrum Automation Manager pane on the Integration window of CA Workload Automation AE Administrator. For more information about configuring CA Workload Automation AE to work with CA Spectrum Automation Manager on Windows, see the *Online Help*.

Chapter 22: Upgrading to the Current Release

This chapter describes how to upgrade from Unicenter AutoSys JM 4.5 through r11 (including service packs) to the current release. These are the only upgrades supported in this release.

The scheduler in the current release can run jobs on the agents for Unicenter AutoSys JM 4.5 through r11 (including service packs). You must upgrade all other CA Workload Automation AE components (including the scheduler, application server, and client) to the current release. Additionally, your database must be compatible with the current release.

Note: After you migrate a database to the new release of CA Workload Automation AE, the original database is not changed.

This section contains the following topics:

Upgrade Considerations

The following are important considerations when upgrading CA Workload Automation AE:

- The installation location you specify for the current release should be different from the Unicenter AutoSys JM 4.5 or r11 installation location.
- The scheduler for the current release can run jobs on the agents for Unicenter AutoSys JM 4.5 through r11 (including service packs). You do not have to upgrade the agents, but you must upgrade all other CA Workload Automation AE components (including the scheduler, application server, and client) to the current release. Additionally, your database must be compatible with the current release.

- You can choose to migrate a Unicenter AutoSys JM database to the current release level of CA Workload Automation AE. However, if you do not choose to migrate your data during the upgrade, you must manually migrate the data after the upgrade process finishes.

  Note: The option to migrate your data during the upgrade is available only if you have Unicenter AutoSys JM 4.5 or r11 installed on the same machine where you are installing the current release. If you are installing the current release on a different machine, then you must migrate your database manually.

- If you use the SSL authentication and encryption option, you can use a single multiplexing port that makes firewall administration easy and minimizes the conflicts with other applications.
- You will be asked for the following information during the upgrade and migration process:
  - Source database machine host
  - Source database name
  - Source TCP/IP port number
  - Source CA Workload Automation AE database user password
  - Source Java JDBC jar file path and file name
  - Target TCP/IP port number

More information:

Upgrade Unicenter AutoSys JM 4.5 or r11 to the Current Release (see page 299)

How the Upgrade Process Works

Upgrading from Unicenter AutoSys JM 4.5 through r11 (including service packs) to the current release requires the following steps:

1. Back up custom data.
2. Upgrade the software to the current release.

   Note: During the upgrade, you can choose to automatically migrate the data.

Upgrade Unicenter AutoSys JM 4.5 or r11 to the Current Release

You can use the provided installation media to upgrade Unicenter AutoSys JM 4.5 or r11 on a UNIX computer.

To upgrade Unicenter AutoSys JM on a UNIX computer

1. Log in as root and shut down all Unicenter AutoSys JM components.
2. Insert the installation media into the drive and mount it.
3. Change directories to the mounted file system and run the installation program using the following command:

   ```
   ./wa_setup.sh
   ```

   The Installation Wizard Welcome page appears.

   Note: You can click Cancel at any time to quit the upgrade. If you click Cancel, the Exit Setup page appears. Click Yes to quit the installation or No to continue the upgrade. If the upgrade is terminated, the Unicenter AutoSys JM instance will not be upgraded.
4. Click Next.

   The Installation Option page appears.
5. Select Upgrade and click Next.

   The Configured Instances page appears.
6. Select the appropriate Unicenter AutoSys JM instance to upgrade, and click Next.

   A confirmation page appears to verify that you want to upgrade.
7. Click Next.

   The Components page appears.

8. Select the components to install, and click Next.
9. Continue with the installation by entering the required information in each wizard page and clicking Next until the Database Type page appears.
10. Select the database type. If you want to migrate the Unicenter AutoSys JM 4.5 or r11 data to the CA Workload Automation AE r11.3 database during the installation process, click the Migrate AutoSys 4.5 or r11 data to the CA Workload Automation AE r11.3 database check box. If you will be using dual event servers, click the Employ dual event servers check box. Then, click Next.

    The Primary Event Server Properties page appears.
11. Specify the primary event server information, which will differ depending on the database type that was selected in Step 10, and do one of the following:

    - If you selected Oracle as the database type, go to the Specify Oracle Database Properties (see page 301) section to continue.
    - If you selected Sybase as the database type, go to the Specify Sybase Database Properties (see page 303) section to continue.

    When you have finished with the database section, continue with Step 12.
12. Specify scheduler, agent, and data encryption information, and click Next.

    If you selected the Migrate AutoSys 4.5 or r11 data to the CA Workload Automation AE r11.3 database check box, the Data Migration – Source Information page appears. Otherwise, the Review Settings page appears, listing the information you entered. In that case, you can proceed to Step 16.
13. Specify the information needed to connect to the Unicenter AutoSys JM 4.5 or r11 database (the source database), and click Next.

    The Data Migration – Target Information page appears.
14. Specify the information needed to migrate the data to the CA Workload Automation AE r11.3 database (the target database), and click Next.

    A preliminary test is made to verify the source and target information you provided. If the information is correct, the Owner and Group Settings page appears. Otherwise, the results of the test are displayed.

    Note: You can click Back to correct the source or target information and then click Next again to verify the information.
15. Specify the system owner and group information that will be assigned to the CA Workload Automation AE r11.3 files when they are installed, and click Next.

    The Review Settings page appears, listing the information you entered.

16. Review the information and, if it is correct, click Next.

    Note: To make a change to an entry, click Back as many times as necessary to locate that entry. Then, make the appropriate change, click Next until the Review Settings page reappears, verify the change, and click Next again.

    The Installation Progress page appears and the progress is displayed. When the installation completes, the Installation Complete page appears.

    Note: The installation and migration process can take from one hour to many hours, depending upon the database type and the amount of data to migrate.

17. Click Finish, then log out and log back in to the CA Workload Automation AE environment.

    The current release of CA Workload Automation AE is installed.

After the upgrade to the current release is complete and you no longer require the prior release of Unicenter AutoSys JM, you can uninstall it.

Note: For information about migrating security policies from Unicenter AutoSys JM 4.5 or r11 (including service packs) to the current release, see the *Security Guide*.

Specify Oracle Database Properties

If you selected the Oracle database on the Database Type page of the installation wizard, you must specify database properties on the appropriate pages in the installation wizard, beginning with the Primary Event Server Properties page.

To specify Oracle database properties

1. Enter the Oracle Service Name, the Oracle Home directory, and the TNS_ADMIN directory. We recommend that you select both the Create or refresh the database and Create the tablespaces check boxes. Click Next.

   The Database Administrator Information page appears.

2. Enter the Oracle Administrator user name and password, and click Next.

   The Database Test page appears.

3. Click Test to verify the existence of the Oracle database and the validity of the connection information.

   The results of the test are displayed.

4. If the test is successful, click OK.

   The Database User Information page appears.

   Note: If the test fails, click Back to correct the connection information.

5. Enter a password for the *aedbadmin* database user and a password for the *autosys* database user, and click Next.

   One of the following occurs:

   - If you selected the Create or refresh the database or Create the tablespaces check boxes on the Primary Event Server Properties page, the Database Tablespace Information page appears. Continue with Step 6.
   - If you selected the Employ dual event servers check box on the Database Type page, the Second Event Server Properties page appears. Continue with Step 7.
   - If you did not select the Create or refresh the database, Create the tablespaces, or Employ dual event servers check boxes, the Scheduler Properties page appears. Continue with Step 12.

6. Specify the data and index tablespace names. If you selected the Create the tablespaces check box, specify the tablespaces sizes (in megabytes) and the directory in which to create the tablespaces, and click Next.

   One of the following occurs:

   - If you selected the Employ dual event servers check box on the Database Type page, the Second Event Server Properties page appears. Continue with Step 7.
   - If you did not select the Employ dual event servers check box on the Database Type page, the Scheduler Properties page appears. Continue with Step 12.

7. Enter the Oracle Service Name for the second event server, select whether to create a database and tablespaces, and click Next.

   The Database Administrator Information page appears.

8. Enter the Administrator user name and password for the Oracle database on the second server, and click Next.

   The Database Test page appears.

9. Click Test to verify the existence of the Oracle database on the second server and the validity of the connection information.

   The results of the test are displayed.

10. If the test is successful, click OK.

    One of the following occurs:

    - If you selected the Create or refresh the database or Create the tablespaces check boxes on the Second Event Server Properties page, the Database Tablespace Information page appears. Continue with Step 11.
    - If you did not select the Create or refresh the database or Create the tablespaces check boxes on the Second Event Server Properties page, the Scheduler Properties page appears. Continue with Step 12.

    Note: If the test fails, click Back to correct the connection information.

11. Specify the data and index tablespace names. If you selected the Create the tablespaces check box, specify the tablespaces sizes (in megabytes) and the directory in which to create the tablespaces, then click Next.

    The Scheduler Properties page appears.

12. Return to the main upgrade procedure and continue with the upgrade.

More information:

Upgrade Unicenter AutoSys JM 4.5 or r11 to the Current Release (see page 299)

Specify Sybase Database Properties

If you selected the Sybase database on the Database Type page of the installation wizard, you must specify database properties on the appropriate pages in the wizard, beginning with the Primary Event Server Properties page.

To specify Sybase database properties

1. Enter the Sybase Server Name, the SYBASE directory path, and the name to use when defining a new Sybase CA Workload Automation AE database, or accessing an existing Sybase database. We recommend that you select both the Create or refresh the database and Create new database devices check boxes. Click Next.

   The Database Administrator Information page appears.

2. Enter the Sybase System Administrator user name and password and specify a password for the *autosys* database user, and click Next.

   The Database Test page appears.

   Note: The Sybase System Administrator user name and password is used when accessing the Sybase Data Server to create the CA Workload Automation AE database. The installation process creates the *autosys* database user if it is not already defined in the database.

3. Click Test to verify the existence of the Sybase database and the validity of the connection information.

   The results of the test are displayed.

4. If the test is successful, click OK.

   One of the following occurs:

   - If you selected the Create or refresh the database or Create new database devices check boxes on the Primary Event Server Properties page, the Data Device Information page appears. Continue with Step 5.
   - If you selected the Employ dual event servers check box on the Database Type page, the Second Event Server Properties page appears. Continue with Step 6.
   - If you did not select the Create or refresh the database or Create new database devices check boxes or the Employ dual event servers check box, the Scheduler Properties page appears. Continue with Step 13.

   Note: If the test fails, click Back to correct the connection information.

5. Specify the directory in which to create the Sybase data device, the device size (in megabytes), and the data device name. For performance consideration, you can specify a separate device for logging by selecting the Create a log device check box, then click Next.

   - If you selected the Create a log device check box, the Log Device Information page displays. Continue with Step 6.
   - If you selected the Employ dual event servers check box on the Database Type page, the Second Event Server Properties page appears. Continue with Step 7.
   - If you did not select the Employ dual event servers check box on the Database Type page, the Scheduler Properties page appears. Continue with Step 13.

6. Specify the directory in which to create the Sybase log device, the device size (in megabytes), and the log device name, then click Next.

   - If you selected the Employ dual event servers check box on the Database Type page, the Second Event Server Properties page appears. Continue with Step 7.
   - If you did not select the Employ dual event servers check box on the Database Type page, the Scheduler Properties page appears. Continue with Step 12.

7. Enter the Sybase Server name for the second event server, enter the database name, and select whether to create a CA Workload Automation AE Sybase Management database and devices, then click Next.

   The Database Administrator Information page appears.

8. Enter the Administrator user name and password for the Sybase database on the second server, and click Next.

   The Database Test page appears.

9. Click Test to verify the existence of the Sybase database on the second server and the validity of the connection information.

   The results of the test are displayed.

10. If the test is successful, click OK.

    - If you selected the Create or refresh the database or Create new database devices check boxes on the Second Event Server Properties page, the Data Device Information page appears. Continue with Step 11.
    - If you did not select the Create or refresh the database or Create new database devices check boxes on the Second Event Server Properties page, the Scheduler Properties page appears. Continue with Step 13.

    Note: If the test fails, click Back to correct the connection information.

11. Specify the directory in which to create the Sybase data device, the device size (in megabytes), and the data device name. For performance consideration, you can specify a separate device for logging by selecting the Create a log device check box, then click Next.

    If you selected the Create a log device check box, the Log Device Information page displays. Continue with Step 12. Otherwise, the Scheduler Properties page appears. Continue with Step 13.

12. Specify the directory in which to create the Sybase log device, the device size (in megabytes), and the log device name, then click Next.

    The Scheduler Properties page appears.

13. Return to the main upgrade procedure and continue with the upgrade.

More information:

Upgrade Unicenter AutoSys JM 4.5 or r11 to the Current Release (see page 299)

Define the localhost Machine After an Upgrade or Database Migration

In previous releases of CA Workload Automation AE, you did not have to define the localhost (the machine where the scheduler started) as a machine in the database. In the current release, you must define all machines where jobs run, including the localhost machine, using the insert_machine JIL command.

Therefore, after you upgrade CA Workload Automation AE or manually migrate the database, you must define the localhost machine. Otherwise, the migrated job definitions that include the **machine: localhost** attribute will not run because CA Workload Automation AE cannot find an associated machine definition.

To define the localhost machine after an upgrade or database migration

1. Run the scheduler, open the scheduler log, and search for the CAUAJM_W_10109 message.

   The message indicates which machine the scheduler is trying to resolve as the localhost.

2. Enter **jil** at the UNIX operating system prompt or the Windows instance command prompt.

   The JIL command prompt is displayed for the local CA Workload Automation AE instance.

3. Specify the following definition:

   ```
   insert_machine: machine_name
   node_name: address
   type: type
   ```

4. Specify optional attributes:

   - agent_name
   - character_code
   - description
   - encryption_type
   - factor
   - heartbeat_attempts (CA Workload Automation Agent for UNIX, Linux, Windows, i5/OS, or z/OS only)
   - heartbeat_freq (CA Workload Automation Agent for UNIX, Linux, Windows, i5/OS, or z/OS only)
   - key_to_agent
   - max_load
   - opsys
   - port

5. Enter exit.

   The data is loaded into the database. The localhost machine is defined in the database.

6. Refresh the scheduler log and look for the CAUAJM_I_10116 message.

   The message confirms that the scheduler resolved the localhost value to the machine defined in Step 2. The scheduler can run jobs on that localhost machine.

Alternatively, instead of defining a new machine, you can set localhost to any existing machine definition. The job definitions that include the machine: localhost attribute will run on that existing machine. To change the localhost setting on UNIX, modify the LocalMachineDefinition parameter in the configuration file. On Windows, modify the Local Machine Definition field in the Scheduler window of CA Workload Automation AE Administrator (autosysadmin).

Note: For more information about the insert_machine subcommand and the related attributes, see the *Reference Guide*.

Example: Define the localhost Machine After a Database Migration

Suppose that the following job definition was migrated from a previous release of CA Workload Automation AE:

```
insert_job: h1
job_type: C
command: ls
machine: localhost
owner: root@localhost
```

After you run the scheduler, the scheduler log contains a message similar to the following:

```
CAUAJM_W_10109 Please define a single machine with the name 'prod' or specify an existing machine as the LocalMachineDefinition configuration variable.
```

This message indicates that the scheduler tried to resolve the localhost to the prod machine. To run the job in the current release, you must define the prod machine in the database. Assuming that the prod machine has a CA Workload Automation Agent installed, the machine definition can be similar to the following:

```
insert_machine: prod
type: a
```

After you define the prod machine, the scheduler log contains a message similar to the following:

```
CAUAJM_I_10116 Localhost machine definition has been successfully set to prod.
```

The job can now run on the prod machine.

Chapter 23: Migrating the Database Manually

Note: This chapter is relevant to Unicenter AutoSys JM 4.5 through r11 (including service packs) to the current release.

If you bypassed the database migration when upgrading your components, follow the appropriate migration procedures in this chapter for your existing release of the database.

Important! Data migration to the current release should be complete before starting any CA Workload Automation AE service of the current release.

This section contains the following topics:

Migration Utility

Unlike in previous releases, the Unicenter AutoSys JM r11 (including service packs) database schema was uniquely identified in a large MDB that included the schemas of many CA products. All CA Workload Automation AE tables were prefixed with ujo_. For example, the job_cond table in Unicenter AutoSys JM 4.5 and 4.5.1 was renamed ujo_job_cond in Unicenter AutoSys JM r11 (including service packs). Additionally, the Unicenter AutoSys JM r11 (including service packs) schema included new tables and new columns in existing tables, and was updated to delete unneeded tables. The current release expanded on those changes and added tables for the newly supported job types. In addition, the current release consolidated the schema into a form that is more normalized. As a result of these changes, upgrading data from previous releases to the current release requires a migration process that retrofits the old data into the corresponding new tables and columns.

The migration utility, which comprises a single JAR file and dynamic library on the CA Workload Automation AE installation media, is written in Java using the Java Database Connectivity (JDBC) API. This utility migrates data in the following instances:

From 4.5.1 or r11 (including service packs) Schema	To the Current Schema
Sybase 11.9.2, 11.9.3, 12.0, or 12.5	Sybase 12.5.2 or 15.0
Oracle 8.17, 9.2, 10g, or 11g	Oracle 9.2, 10g, or 11g

Note: For more information about supported database versions, check the CA Workload Automation Support web page at http://ca.com/support.

The CA Workload Automation AE migration utility is invoked by a Perl script that takes a file name as a parameter. The input file contains the list of parameters that specify the credentials of the source database (the Unicenter AutoSys JM 4.5.1 or r11 (including service packs) instance) and the target database (the current CA Workload Automation AE instance). You can invoke the utility from the computer that the current instance is installed on. Because the utility is based on JDBC, it does not mandate the existence of database-specific client or server software on the computers involved.

Pre-Migration Considerations

The following information should be considered before starting the migration process:

- Migrating large amounts of data will take a considerable amount of time. We recommend scheduling the migration accordingly.
- We recommend archiving old information from the database using archive_events on the old instance before invoking the migration utility. This will reduce the amount of data that needs to be migrated and will be more time-efficient.
- Superuser information will be migrated from Unicenter AutoSys JM r4.5.1 only if that instance is using native security. Unicenter AutoSys JM r11 (including service packs) superuser information will be migrated if the instance is using native security or CA EEM for security. However, you can still use the autosys_secure utility in the current release to set up superuser information. After migrating from an instance that is using CA EEM for security, it is necessary to regenerate the security certificate for CA Workload Automation AE either with the as_safetool or the CA EEM GUI.
- We recommend creating a new parameter file using the one supplied with the installation, to ensure that you have the correct information for your migration. When the migration is complete, delete the parameter file or change the CA Workload Automation AE user password in the parameter file to avoid a security exposure on the CA Workload Automation AE user password, which is stored in ASCII format.
- The source database remains intact during the migration process with the exception of Oracle. If the source and target instances are using the same Oracle installation, several global synonyms are replaced, causing the previous definitions to be replaced. The list of objects with global synonyms is as follows: send_event, alamode, event, intcodes, proc_event, and timezones.
- We recommend gathering the following data before invoking the migration utility. You will need this information to complete the migration utility parameter file.
  - TCP/IP Database Listener Port Number
  - Native JDBC JAR Path
  - Database JAR File

More information:

Locating the TCP/IP Database Listener Port Number (see page 312)
Determine the Native JDBC JAR Path (see page 313)
Download Database JAR Files (see page 313)

How to Migrate the Database Manually

To migrate the Unicenter AutoSys JM database manually, follow these steps:

1. Archive old information on the Unicenter AutoSys JM database (see page 312).
2. Locate the TCP/IP database listener port number (see page 312).
3. Determine the native JDBC JAR path (see page 313).
4. Download the database JAR files (see page 313).
5. Invoke the migration utility (see page 314).
6. Stop the migration utility (see page 317).

Archive Information on the Unicenter AutoSys JM Database

To archive information from the Unicenter AutoSys JM 4.5 or r11 database, run DBMaint on the old instance before invoking the migration utility. This will reduce the amount of data that needs to be migrated.

Locating the TCP/IP Database Listener Port Number

The TCP/IP database listener port numbers are required during the migration process to complete the migration utility parameter file, based on your installation. The port numbers facilitate communications across database instances.

Locate the TCP/IP Port for Oracle

To find the TCP/IP port for Oracle, open the tnsnames.ora file typically located in %ORACLE_HOME%\network\admin. Locate the following parameter:

```
(ADDRESS = (PROTOCOL = TCP)(HOST = host.domain.com)(PORT = 1521))
```

Note: The default port number is 1521.

Locate the TCP/IP Port for Sybase

To find the TCP/IP port for Sybase, open the sql.ini file for Adaptive Server Enterprise. The default location is %SYBASE%\ini\sql.ini. Locate the following database entry:

```
[AUTOSYSDB]
MASTER=NLWNSCK,machine1,5000
QUERY=NLWNSCK,machine1,5000
```

Note: The default port number is 5000.

Determine the Native JDBC JAR Path

You must use the NATIVEJDBCJARPATH command in the parameter file to specify the JAR file path for the Oracle and Sybase database types. The following tables list native JDBC JAR files and their example sample paths:

Oracle: Oracle Database 10g JDBC Drivers

JDBC JAR	Example Path
classes12.jar	/oracle/10.1.0/jdbc/lib/classes12.jar
ojdbc14.jar	/oracle/10.2.0/jdbc/lib/ojdbc14.jar

Sybase: Sybase jConnect for JDBC Version 6.0

JDBC JAR	Example Path
jconn3.jar	/sybase/jConnect-6_0/jconn3.jar

Note: The migration utility requires access to these JAR files to perform the migration. Ensure that these sets of drivers are installed and accessible on the installation before proceeding with the migration. The example paths are for illustrative purposes and may not be the same on every installation.

Download Database JAR Files

If you do not have the database vendor JAR file installed, you can download the respective JAR files for each database vendor. Follow the installation instructions as specified by each vendor. Contact the specific vendor for any licensing requirements.

Migrate a Unicenter AutoSys JM 4.5 or r11 Database

If you bypassed the automatic database migration when you upgraded to the current release, you must run the migration utility before you can use your new CA Workload Automation AE instance.

Important! Before using CA Workload Automation AE, you must ensure that data migration is completed successfully. Any data in the target database is removed before the actual migration starts with the exception of CA Workload Automation AE users, which are retained.

To migrate a Unicenter AutoSys JM 4.5 or r11 database

1. Open a CA Workload Automation AE sourced environment.
2. Stop the scheduler and application server.
3. Enter the following command:

   ```
   cd $AUTOSYS/dbobj/DataMover
   ```

   The DataMover directory appears.
4. Do *one* of the following, assuming that CA Workload Automation AE is installed in /opt/CA/WorkloadAutomationAE, the common components are installed in /opt/CA/SharedComponents, and the CA Workload Automation AE instance ID is ACE:

   - Manually update the library search path as follows:

     AIX

     ```
     LIBPATH=/opt/CA/WorkloadAutomationAE/autosys/lib:/opt/CA/SharedComponents
     /lib:$LIBPATH; export LIBPATH
     ```

     HP-UX

     ```
     SHLIB_PATH=/opt/CA/WorkloadAutomationAE/autosys/lib:/opt/CA/SharedCompone
     nts/lib:$SHLIB_PATH; export SHLIB_PATH
     ```

     SunOS

     ```
     LD_LIBRARY_PATH=/opt/CA/WorkloadAutomationAE/autosys/lib:/opt/CA/SharedCo
     mponents/lib:$LD_LIBRARY_PATH; export LD_LIBRARY_PATH
     ```

     Linux

     ```
     LD_LIBRARY_PATH=/opt/CA/WorkloadAutomationAE/autosys/lib:/opt/CA/SharedCo
     mponents/lib:$LD_LIBRARY_PATH; export LD_LIBRARY_PATH
     ```

   - Source the CA Workload Automation AE environment as follows:

     ```
     ./opt/CA/WorkloadAutomationAE/autouser.ACE/autosys.shell.host
     ```

   The library search path is updated.

5. Edit the following parameters in the paramfile file, using values based on your installation:

SRCDBTYPE

Defines the source database type. Valid values are *oracle* and *sybase*.

SRCDBMACHINE

Defines the source database computer.

SRCDBNAME

Defines the source database name.

SRCDBPORT

Defines the source database port (the TCP/IP listener port for the database).

SRCDBUSER

Defines the source database Unicenter AutoSys JM user. For Oracle 11.0, this must be *aedbadmin*.

SRCDBPWD

Defines the source database Unicenter AutoSys JM user password.

TGTDBTYPE

Defines the target database type. Valid values are *oracle* and *sybase*.

TGTDBMACHINE

Defines the target database machine.

TGTDBNAME

Defines the target database name.

TGTDBPORT

Defines the target database port (the TCP/IP listener port for the database).

TGTDBUSER

Defines the target database CA Workload Automation AE user. For Oracle, this must be *aedbadmin*.

TGTDBPWD

Defines the target database CA Workload Automation AE user password. For Oracle, this must be the password for *aedbadmin*.

NATIVEJDBCJARPATH

Defines an Oracle or Sybase JDBC JAR path.

JREPATH

Defines the JRE root path.

Note: The migration utility requires JRE 1.5.0_11, or higher, which is installed by default with CA Workload Automation AE.

- **Example Path on UNIX:**

  /opt/CA/SharedComponents/JRE/1.5.0_11

VERIFY

Note: We recommend that you first set the VERIFY parameter to YES. This will ensure that all the connection information is correct before actually migrating any data.

Specifies whether to verify the source and target credentials. Valid values are:

yes

Tests the source and target credentials and prints a message if the verification test is successful, but does not proceed with the migration. This lets you verify that the input parameters for the source and target databases are correct and perform the data migration later.

no

Continues the migration process without verifying the source and target credentials.

6. Run the uajmdatamover.pl utility using the following command:

   ```
   perl uajmdatamover.pl paramfile
   ```

   A message appears if the verification test is successful.

7. Repeat Step 5, setting the VERIFY parameter to NO.

8. Repeat Step 6.

   The migration utility completes the migration. When the migration is successful, the command prompt returns with a timestamp message. A log of the actions taken is written to DataMover.log in the dbobj directory.

9. Start the scheduler using eventor, run autosys_secure to set the superuser information, and verify that the migration was successful.

   Note: Superuser information will be migrated from prior releases (if they are using native security) or from Unicenter AutoSys JM r11 (including service packs). CA EEM deemphasized the need for superusers.

   Important! The scheduler adjusts CA Workload Automation AE information in the migrated database. You must run the scheduler at least once before you run any other CA Workload Automation AE processes.

Stop the Migration Utility

If for some reason you need to stop the migration utility, you may do so at any time during the migration process.

To stop the migration utility, press Ctrl+C while the utility is running. The following message appears:

User Interrupt Encountered. AutoSys Database Not Migrated.

Please rerun the utility. Exiting...

Re-Invoke the Migration Utility

If the migration process is interrupted, you will need to re-invoke the migration utility later to start the process again.

Sample UNIX Parameter File

The following is an example of a UNIX parameter file, created during the migration process from Unicenter AutoSys JM 4.5 or r11 to the current release.

```
SRCDBTYPE=Sybase
SRCDBMACHINE=machine1
SRCDBNAME=autosys
SRCDBPORT=5001
SRCDBUSER=autosys
SRCDBPWD=autosys
TGTDBTYPE=oracle
TGTDBMACHINE=machine2
TGTDBNAME=aedb
TGTDBPORT=1521
TGTDBUSER=aedbadmin
TGTDBPWD=aedbadmin
NATIVEJDBCJARPATH=/opt/oracle/10.2.0/jdbc/lib/ojdbc14.jar
JREPATH=/opt/CA/SharedComponents/JRE/1.5.0_11
VERIFY=no
```

Appendix A: lsm

This appendix provides information about the lsm command.

lsm Command—Manage UNIX Products on Target Computers

The lsm command lets you manage UNIX products on target computers. These UNIX products can be packaged in one of the following formats:

- PIF (Product Interchange Format)
- PKG (UNIX SVR4 Standard Packaging)
- RPM (Red Hat® Package Manager)

The lsm command provides methods to install, remove, list, backup, check, query installed products, query PIF product files, and update installed products. Therefore, root permission is required on the target computer.

This command has the following format:

```
lsm -i product_file [-r response_file] [-s] [-F] [-I instance]
lsm –e product_name [-s] [-R] [-I instance]
lsm -l [-O pif|rpm|pkg] [-g product_family] [-f file] [-S]
lsm –A product_name –d product_file [-o]
lsm –c product_name
lsm -u product_family -d product_folder [-r response_file]
lsm –q product_name [-l]
lsm –Q product_file [-l]
lsm –a product_file –r response_file
lsm -v
```

-i *product_file* [-r *response_file*] [-s] [-F] [-I *instance*]

Installs a PIF, PKG, or RPM packaged product. You must specify the full path name of the product.

-r *response_file*

(Optional) Identifies the response file that can be added to customize the unattended installation.

-s

(Optional) Runs the installation in unattended mode.

-F

(Optional) Performs a forced installation; that is, if the backup of an existing product fails, the installation continues.

-I

(Optional) Defines a 2-byte instance number in the range of 00 to 99 for the product. On the target computer, the product name is extended with this instance number, as follows: product_name_instance. This extension lets you distinguish different instances of the same product version (in case of multiple installations). Only the specified instance of the PIF product is installed on the target computer.

-e *product_name* [-s] [-R] [-I *instance*]

Removes the specified installed product.

-s

(Optional) Runs the uninstallation procedure in unattended mode.

-R

(Optional) Retains all configuration files on the system.

-I *instance*

(Optional) Defines a 2-byte instance number to identify the product to be removed in case of multiple installations.

-l [-O *pif|rpm|pkg*] [-g *product_family*] [-f *file*] [-S]

Lists products.

O *pif|rpm|pkg*

(Optional) Lists only the installed products of the specified type.

-g *product_family*

(Optional) Lists all products assigned to a specified product family.

-f *file*

(Optional) Lists the product that installed the specified file.

-S

(Optional) Lists all installed products or shared components.

-A *product_name* -d *product_file* [-o]

Creates the backup file (product_file) of the installed PIF or PKG product (product_name).

-o

(Optional) Overwrites an existing product_file.

-c *product_name*

Checks the specified installed product for consistency, that is, the files of the product are checked for existence, and additionally, access, user and owner rights are checked.

-u *product_family* -d *product_folder* [-r *response_file*]

Updates the installed products of a product family.

-q *product_name* [-l]

Queries the installed product (product_name) and displays the product properties.

-l

(Optional) Provides a long list of product properties, including all installed product files.

-Q *product_file* [-l]

Queries the PIF product (product_file), and displays the product properties.

-l

(Optional) Provides a long list of product properties, including all installed product files.

-a *product_file* -r *response_file*

Runs the installation dialogs and creates a response file using the values entered. The PIF product is not installed.

-v

Prints the version of the installer used.

The lsm command exit status is displayed as follows:

```
0 OK
!= 0 Error
```

Example: Install PIF Product CAWorkloadAutomationAE.Linux.@pif on the Local System

This example installs the PIF product CAWorkloadAutomationAE.Linux.@pif on the local system:

```
lsm -i CAWorkloadAutomationAE.Linux.@pif
```

Example: Create a Backup File of the Installed PIF Product CAWorkloadAutomationAE

This example creates a backup file of the installed PIF product CAWorkloadAutomationAE. The backup file has the name auto.bkup, and is located in the /tmp directory:

```
lsm -A CAWorkloadAutomationAE –d /tmp/auto.bkup
```

Appendix B: Removing CA Workload Automation AE

How to Remove CA Workload Automation AE

To complete the uninstallation procedure for CA Workload Automation AE, follow these steps:

1. Uninstall CA Workload Automation AE (see page 323).
2. Remove the database tables and data (see page 324).
3. Delete the auto.profile file (see page 324).

Uninstall CA Workload Automation AE

If necessary, you can uninstall CA Workload Automation AE using the installation wizard.

To uninstall CA Workload Automation AE

1. Log in as root.
2. Mount the CA Workload Automation AE media.
3. Change directories to the mounted file system and run the following command:

   ```
   ./wa_setup.sh
   ```

   The Welcome page appears.
4. Select Remove and click Next.

   The Remove Product page appears.
5. Select the Backup CA Workload Automation AE and restore the old version if the removal fails check box and click Next.

   The Remove Product page appears, listing the components that will be removed.

   Note: CA Common Services components are removed unless they are being used by another product.
6. Click Remove.

   The Monitor Progress page appears and the progress is displayed. When the update completes, the Deinstallation Complete page appears.
7. Click Ok.

   The product is uninstalled.

Remove the Database Tables

After CA Workload Automation AE is uninstalled, you must remove the database tables and data. The uninstallation process copies the database removal script in the /tmp ($TMPDIR) directory.

To remove the database tables and data

1. Run the following command from the /tmp ($TMPDIR) directory:

   `./rm_waae_p`*`ACE`*`.sh`

   ACE

   Specifies the instance that was created when CA Workload Automation AE was installed.

   You will be prompted for the database connection information.

   Note: Default values are supplied based on the installed database type (Oracle or Sybase).

2. Continue by entering the required information at each prompt and pressing Enter.

   The existing CA Workload Automation AE database tables, roles, and users are removed.

3. (Optional) Repeat Steps 1 and 2, using the following command in place of the p*ACE* command in Step 1, only if you installed dual event servers:

   `./rm_waae_s`*`ACE`*`.sh`

   The data is removed from the second event server.

(Sybase only) **Note:** You must remove the Sybase device files, which are in the directory specified in the Sybase Data and Log Directories. For example, if the device files are in /opt/sybase/data, run the following commands:

```
cd /opt/sybase/data
rm –f AEDB_DATA.DAT
rm –f AEDB_LOG.DAT
```

Delete the auto.profile File

After CA Workload Automation AE is uninstalled, you must manually delete the auto.profile file from the /etc directory.

Index

D

E

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Z