CA Workload Automation AE

Windows Implementation Guide

r11.3

ca technologies

This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

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 4: Installation Considerations 49

Chapter 5: Installing the Server 55

Chapter 6: Installing the Client 83

Chapter 7: Installing the Agent 91

Chapter 8: Setting Up the Database Manually 105

Chapter 9: Installing the SDK Runtime Environment 125

Chapter 10: Installing the Server, Client, or Agent Silently 129

Chapter 11: Post-Installation Procedures for the Server 133

Chapter 12: Modifying an Existing Installation 139

Chapter 13: Configuring CA Workload Automation AE to Work with the Agent 143

Chapter 14: Configuring CA Workload Automation AE to Work with CA Common Components 179

Chapter 20: Configuring CA Workload Automation AE to Work with Other CA Products 279

Chapter 21: Upgrading to the Current Release 293

Chapter 22: Migrating the Database Manually 307

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 upgrading an existing installation, adding CA Workload Automation AE superusers, and setting the Windows user IDs and passwords.

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 Windows. It assumes familiarity with the operating system and with the database server you use.

Note: The term *Windows* refers to any Microsoft Windows operating system supported by CA Workload Automation AE.

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.

Command Syntax Conventions

The conventional Windows instance command prompt commands have the following format:

```
name [option...] [command argument...]
```

For example:

```
x_stgd -h [-l [level]] [-L file] [-a port] [-d [level]][-s server] [-m hostname]
[-S status] [action -P|-R -p {-T -H -y}]
```

The following are the command syntax conventions:

- Options consist of one character and are always preceded by a hyphen (-).
- Options with no arguments can be grouped after a single hyphen.
- Brackets [ ] surround an option or command argument that is optional.
- Braces {} enclose options or arguments that are interdependent; everything enclosed must be treated as a unit.

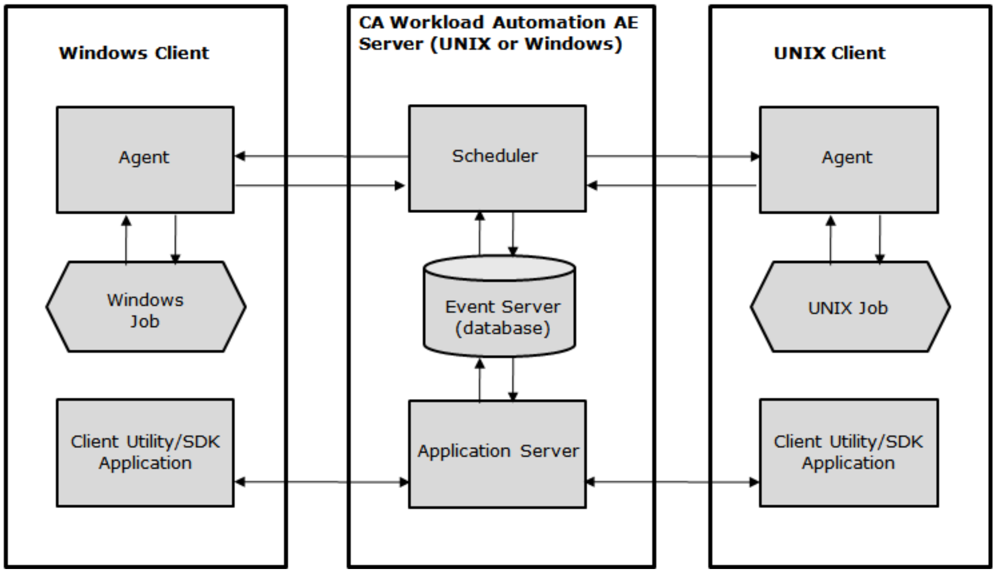
CA Workload Automation AE Components

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:


Windows Client
Agent
Windows Job
Client Utility/SDK Application
CA Workload Automation AE Server (UNIX or Windows)
Scheduler
Event Server (database)
Application Server
UNIX Client
Agent
UNIX Job
Client Utility/SDK Application

Event Server

The *event 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 25)

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

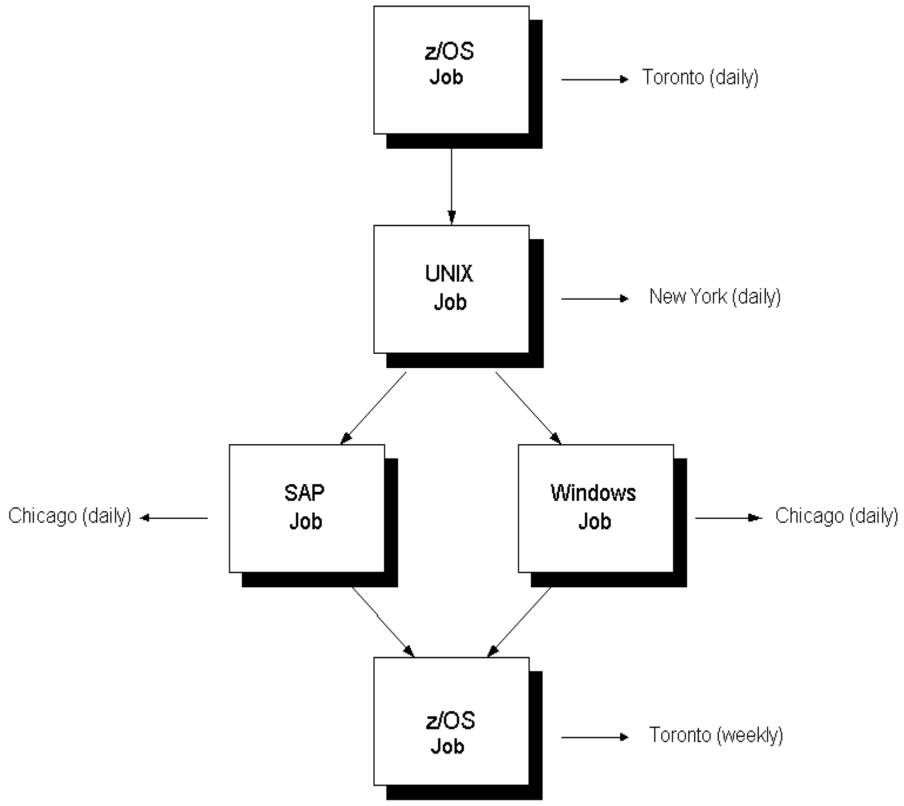
Agents are the key integration components of CA workload automation products. Agents let you automate, monitor, and manage workload on all major platforms, applications, and databases. To run workload on a particular system, you install an agent on that system. If your workload must run on a UNIX computer, 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 Workload Control Center (CA WCC) to define, monitor, and report on jobs.

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

CA Workload Automation AE also provides CA Workload Automation AE Administrator, which lets you view or modify the configuration parameters of all the CA Workload Automation AE instances that you have installed. You can also define the job profiles that contain the environment variables that must be set for a job to run.

Note: For more information about how to view or modify the configuration parameters of a CA Workload Automation AE instance on Windows using CA Workload Automation AE Administrator, see the Online Help.

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:

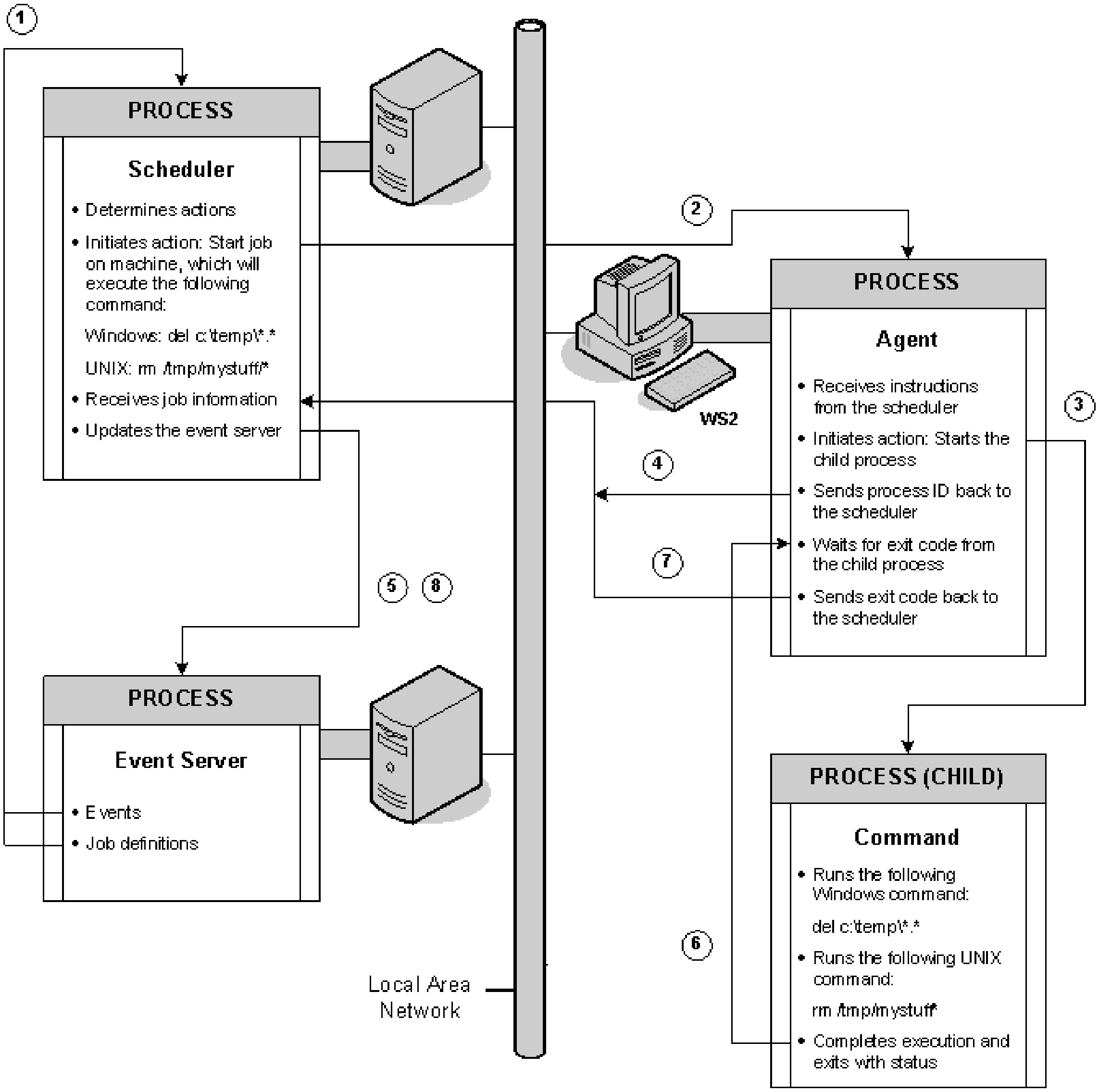
     ```
     del C:\tmp\*.*
     ```

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):


1
PROCESS
Scheduler
• Determines actions
• Initiates action: Start job on machine, which will execute the following command:
Windows: del c:\temp\*.*
UNIX: rm /tmp/mystuff/*
• Receives job information
• Updates the event server
2
PROCESS
Agent
• Receives instructions from the scheduler
• Initiates action: Starts the child process
• Sends process ID back to the scheduler
• Waits for exit code from the child process
• Sends exit code back to the scheduler
WS2
3
4
7
5
8
PROCESS
Event Server
• Events
• Job definitions
PROCESS (CHILD)
Command
• Runs the following Windows command:
del c:\temp\*.*
• Runs the following UNIX command:
rm /tmp/mystuff*
• Completes execution and exits with status
6
Local Area Network

Notes:

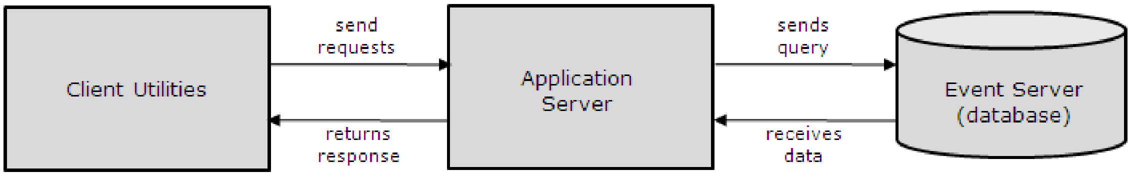
- The application server communicates with the agent only when client utilities like chase and autoping are run or when jobs contain globs or blobs as input or output.
- The scheduler and the event server typically run on the same computer.

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. You can specify a different ID during installation only.

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 using the installation wizard.

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 *server* 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.

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.

Note: You can configure the high availability options on Windows using CA Workload Automation AE Administrator. For more information about CA Workload Automation AE Administrator, see the *Online Help*.

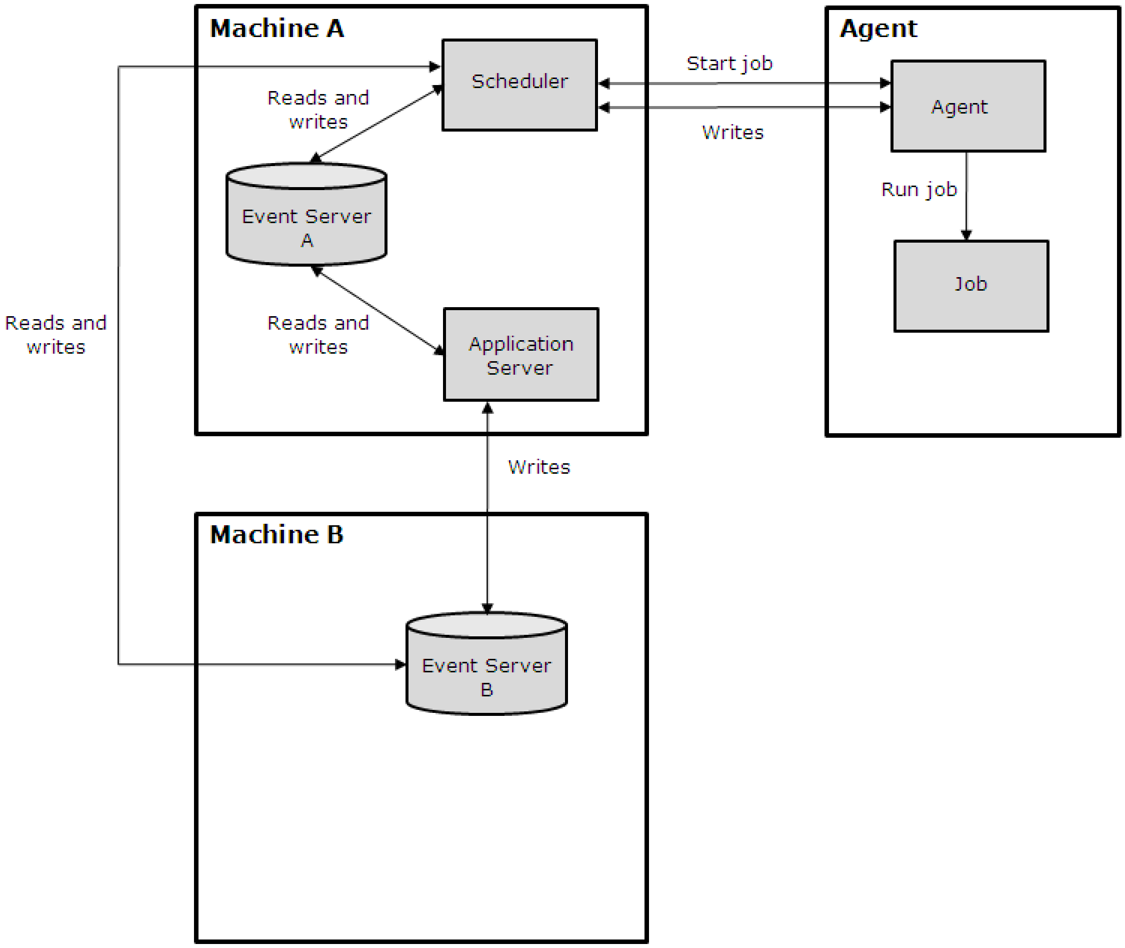
Dual Event Servers

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.

When CA Workload Automation AE is running with dual event servers and one of the servers goes down, the Event Server - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator on the scheduler computer shows that one event server’s status is DOWN, selects the A Database Rollover Has Occurred check box, and marks the remaining event server as being in single event server mode. These changes indicate to you and the utilities attempting to access the database that CA Workload Automation AE is running in single event server mode so that client processes will not attempt to write to the event server which is down.

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.

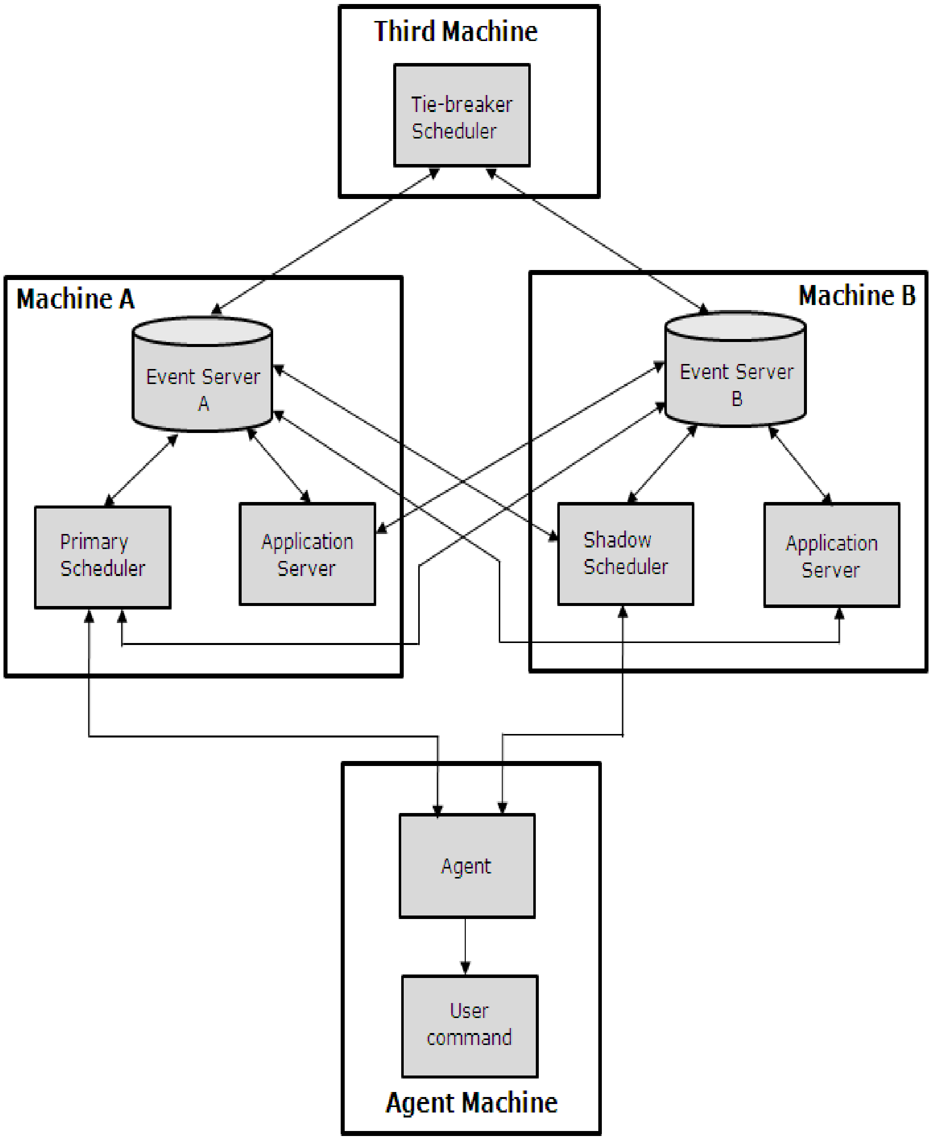
Before restarting the server that is down, you must make sure that the two event servers are synchronized.

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*.

Highly-Available Cluster Environment

CA Workload Automation AE can be installed in a Microsoft Cluster Server Environment to form a highly-available CA Workload Automation AE scheduler and application server. The CA Workload Automation AE highly-available configuration promotes minimal down time and uses resources optimally to ensure that your enterprise is continuously monitored and managed.

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:

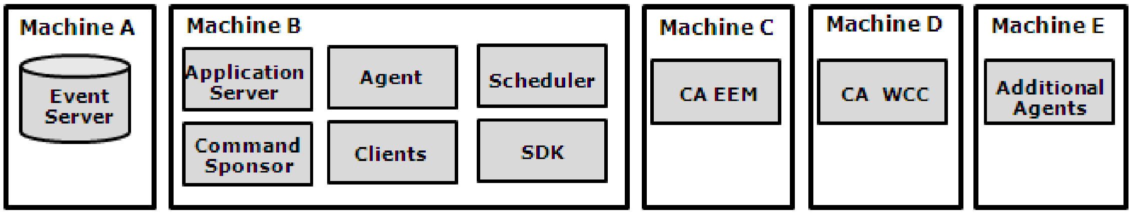
- You can perform the tasks listed in the table if you are installing CA Workload Automation AE for the first time or installing CA Workload Automation AE in a test environment before upgrading and migrating your data to the current release.
- We recommend that you install the CA products in the order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

Installation Phase	Tasks to Perform
Pre-Installation	Plan your environment (see page 31)
	Get the required CA Workload Automation AE licenses (see page 31)
	Set up the database for CA Workload Automation AE (see page 32)
Installation	Install CA EEM (see page 32)

Installation Phase	Tasks to Perform
	Install and verify the CA Workload Automation AE server (see page 33) **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 Installation Considerations (see page 49)
	Install, configure, and verify CA WCC (see page 33)
	Install and verify additional agents on other computers (see page 34)
	Install and verify agent plug-ins (see page 34)
Post-Installation	Install the required patches (see page 34)
	Set up custom CA EEM security policies (see page 35)

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 46).

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 57).

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 38)
- Host Machine Checklist (see page 47)
- Installing into an Existing MDB (Oracle Only) (see page 50)
- Installing CA Workload Automation AE with Sybase (see page 51)
- Installing CA Workload Automation AE with Oracle (see page 52)
- Configure the Environment to Use a 64-bit Database (see page 53)

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 55).
- You can verify the CA Workload Automation AE server installation by running a test job. For more information, Running a Test Job (see page 79).

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 CA SDM or the silent installation files to install additional agents on other computers. For more information about installing the agent silently, see Installing the Server, Client, or Agent Silently (see page 129).
- 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 91). 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 143).

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.

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 Oracle, Microsoft SQL Server, or Sybase database, CA Workload Automation AE relies on the environment variables. For Windows, these variables are set during installation, and you can view the settings on the System - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.

Note: For more information about the CA Workload Automation AE Administrator, see the *Online Help.*

More information:

Database-specific Environment Variables (see page 38)

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.

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). The application server and scheduler computers require a database client to connect to the event server.

More information:

Database Connection (see page 40)

Microsoft SQL Server

For Microsoft SQL Server, you must install the Microsoft SQL Server client utilities on each scheduler and application server computer. Then, you must make sure that there is database connectivity between the event server, scheduler, and application server computers. When you install CA Workload Automation AE, you must indicate the appropriate event server information, including the event server name (Microsoft SQL Server name) and database name.

In addition, you must meet Microsoft SQL Server security requirements for CA Workload Automation AE database users.

Note: For CA Workload Automation AE to support Microsoft SQL Server, mixed mode authentication must be enabled.

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.

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.

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.

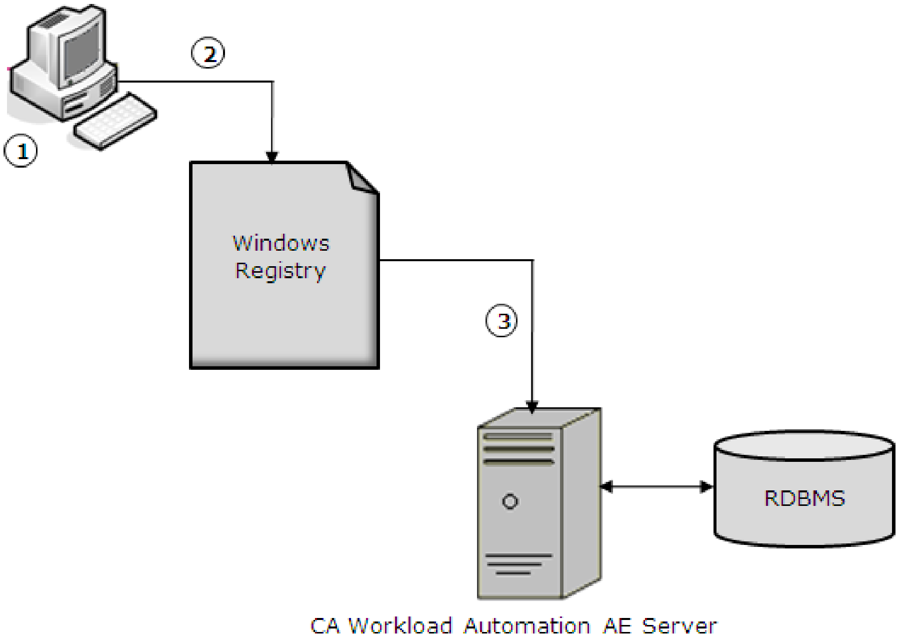
More information:

How CA Workload Automation AE Connects to a Microsoft SQL Server Database (see page 41)
How CA Workload Automation AE Connects to an Oracle Database (see page 42)
How CA Workload Automation AE Connects to a Sybase Database (see page 43)

How CA Workload Automation AE Connects to a Microsoft SQL Server Database

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

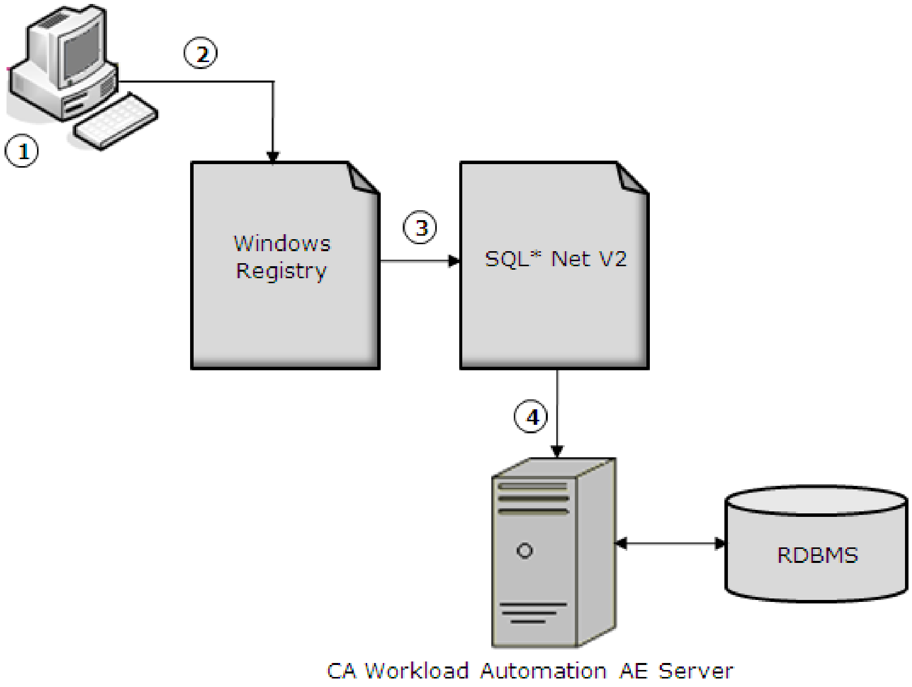
1. Reads the CA Workload Automation AE Administrator settings in the Windows Registry to locate the event server and database configuration settings. For example: AEDB user:autosys.
2. Uses an internally built open database connectivity (ODBC) connection to connect to the database. It needs to know the Microsoft SQL Server name or servername/instance and the Microsoft SQL Server database name.



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:

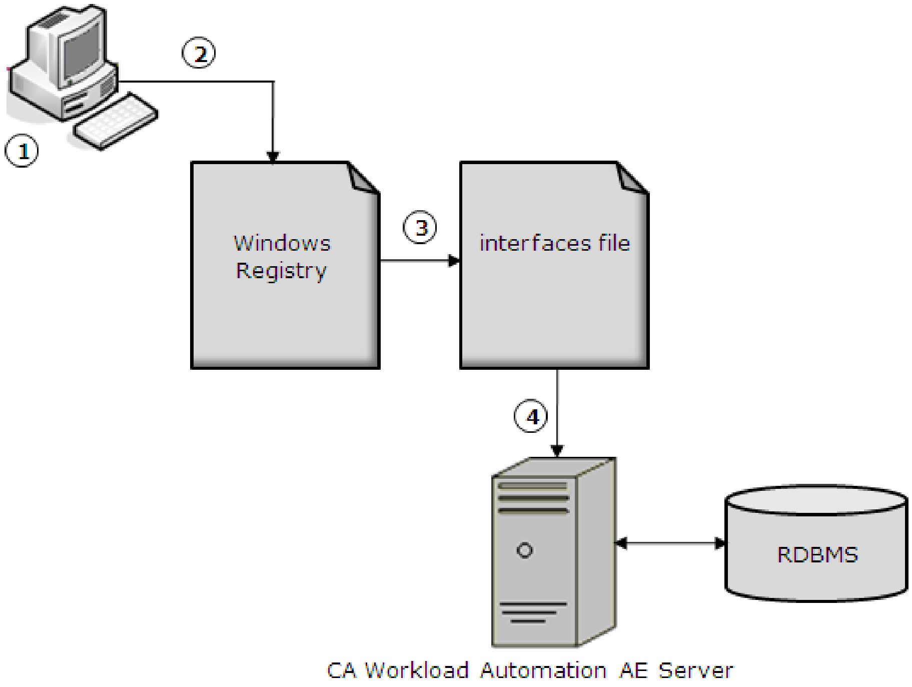
1. Reads the CA Workload Automation AE Administrator settings in the Windows Registry to locate the event server and database configuration settings. For example: AEDB user:autosys.
2. Searches for the TNS alias MYORACLEDB in the tnsnames.ora file.
3. Uses network configuration information to connect 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 CA Workload Automation AE Administrator settings in the Windows Registry to locate the event server and database configuration settings. For example: AEDB user:autosys.
2. Searches for AEDB in the interfaces file.
3. Uses the host name and port number entry to connect to the database.



Multiple Instances

Multiple instances of CA Workload Automation AE are supported and these instances will share the %AUTOSYS% directory. Only a new %AUTOUSER% directory will be created.

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 %TEMP% environmental variable that refers to a valid directory on the installation computer.

The setup program creates a log file in the c:\%TEMP% directory called WAAE_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 install log is created in the %TEMP% 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*.

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 Requested	Your Selection or Value
Platform	
Operating system/version	
Host name	
Minimum requirements—Available memory (1 GB)	
Minimum requirements—Available disk space (1 GB)	
Instance name (AUTOSERV)	
Name of data server that contains the database	
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, agent, or both. You can define an agent computer to run jobs only, or a client computer to run both the jobs and the GUIs 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*.

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 and Event Management

Consider the following when installing CAICCI (CA, Inc. Common Communications Interface) and Event Management on Windows:

- We recommend that you stop all Windows programs, including antivirus software packages, before installing CAICCI and Event Management for CA Workload Automation AE.
- The Windows account used to install CAICCI and Event Management for CA Workload Automation AE must have administrative rights.
- You must install CAICCI and Event Management for CA Workload Automation AE from either the supplied DVD or from a local hard disk. If you install CAICCI and Event Management for CA Workload Automation AE from the local hard disk, the entire DVD image must be copied to a folder under the root of a drive on the local machine.

  Note: Due to restrictions in some of the CA common components, do not include spaces in this folder name.

- 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 Windows, if you uninstall a previous CA Workload Automation AE release that installed CAICCI, CAICCI also may be uninstalled. In this case, the user definitions are retained in a file named ccirmtd.rc.bak, located in <CCI>/CAIUSER. If CAICCI is installed using the CA Common Components DVD, the definition file resides in the CA_APPSW folder. Use the command cci_config_locator.exe to determine where the current ccirmtd.rc file is located. To migrate the previous user definitions, you can rename ccirmtd.rc.bak to ccirmtd.rc and replace the copy of the file in the CA_APPSW folder.

Installing CA EEM

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

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:

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;
```

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 and perform additional configuration tasks. Do these procedures before you install CA Workload Automation AE.

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:
   - Permanently modify the Windows path environment variable as follows:
     a. In the Windows path environment variable, ensure that the path to the 32-bit client bin directory precedes the path to the 64-bit client bin directory.
     b. Install the CA Workload Automation AE server.
   - If you cannot permanently modify the Windows path variable, do the following:
     a. Modify the path for the local environment before you run the CA Workload Automation AE installation program.
     b. Install the CA Workload Automation AE server.
     c. Modify the path variable in the Administrator utility for CA Workload Automation AE (see page 54).

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

Modify the Path Environment Variable in the Administrator Utility

In the Windows system path, the 32-bit client bin directory for the database must precede the 64-bit client bin directory. If you cannot permanently modify the Windows system path, modify the path variable in the Administrator utility after you install CA Workload Automation AE. The variables defined in the Administrator utility set the environment for CA Workload Automation AE.

To modify the path environment variable in the Administrator utility

1. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select the name of your CA Workload Automation AE instance from the Instance drop-down list.

3. Click the System icon on the toolbar.

   The System - CA Workload Automation AE Administrator window appears.

4. Double-click PATH in the Environment Variables pane.

   The window refreshes to display PATH in the Variable field and its value in the Value field.

5. Enter the path to the 32-bit client libraries for your database in the Value field, and click Set.

   Note: Ensure that the path to the client libraries precedes the %PATH% variable.

   The PATH variable definition is modified and displayed in the Environment Variables pane. CA Workload Automation AE is configured to use the 64-bit version of Oracle, Sybase, or Microsoft SQL Server.

Chapter 5: Installing the Server

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

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—C:\Program Files\CA\WorkloadAutomationAE on 32-bit operating systems or C:\Program Files (x86)\CA\WorkloadAutomationAE on 64-bit operating systems.
  - CA common components—C:\Program Files\CA\SC or C:\Program Files\CA\SharedComponents on 32-bit operating systems, or C:\Program Files (x86)\CA\SC or C:\ Program Files (x86)\CA\SharedComponents on 64-bit operating systems.
  - Shared Files—C:\Program Files\CA\CA_APPSW or C:\CA_APPSW

  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 not use the same installation directory name that you used in a previously installed Unicenter AutoSys JM 4.5 or r11. 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. If you select to perform a Standalone installation, it lets you do the following:
  - Create the database.
  - Migrate the database.
- 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*.

More information:

How to Install the Server (see page 58)
Installation Checklist for the CA Workload Automation AE Server (see page 59)

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 at C:\Program Files\CA\SharedComponents\CA_LIC 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 database. The supported databases are Oracle, Sybase, and Microsoft SQL Server.
2. Collect the required information (see page 59).

   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 70).
4. Define the agent on the server (see page 71).
5. Verify the installation (see page 71).

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 46) installed during a typical server installation are as follows:

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

Note: After you have answered the questions in this checklist, see the host machine checklist and complete it.

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

Information Requested	Installation Type	Your Selection or Value
Installation Path The preferred installation drive. The CA Workload Automation AE installation path. The default installation path is C:\Program Files\CA\Workload Automation AE. The CA Shared Directory installation path. The default installation path is C:\Program Files\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 to encrypt data using the default or a user-specified key. The Encrypt data using Workload Automation default encryption key option is selected by default. If you select Encrypt the data using a user-specified 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 Properties 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. The application server auxiliary listening port. The default port number is 7500. (Typical only) The scheduler auxiliary listening port. The default port number is 7507. The application server settings: ■ 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 only) Whether you want to configure the CA Workload Automation AE instance for a highly-available cluster environment. **Note:** By default, the Configure this instance for a highly-available clustered environment check box is disabled. It is enabled only if you run CA Workload Automation AE in a cluster environment. ■ (Custom only) Whether you want the application server to start automatically at system startup time. This check box is selected by default. ■ (Custom only) Whether you want the application server to start immediately after installation. This check box is selected by default.	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
CA Embedded Entitlement 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 Properties 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	
Agent Information The agent name. The default agent name is WA_AGENT. The agent port number. The default port number is 7520. If port multiplexing is selected, the default port number is 49154. The agent settings: ■ 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.	Typical or 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.	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
CA Workload Automation Database Properties The database type for the CA Workload Automation AE instance. The available database types are Microsoft SQL Server, 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	
Note: The next several rows in this table describe the Microsoft SQL Server pages. If you have selected Oracle or Sybase, you can skip to the Oracle or Sybase rows in this table.		
Microsoft SQL Server Only		
Primary Event Server Properties The event server settings: ■ Whether you want to create the CA Workload Automation AE database. This check box is selected by default. ■ The logical name of the database server. The name of the host computer where the server is installed is the default. ■ The name of the database. The default database name is AEDB. ■ Whether you want to use Windows authentication. This option is selected by default. ■ Whether you want to use SQL Server authentication. If you select this option, you must specify the SA user name and password.	Typical or Custom	
Primary Event Server Properties CA WAAE Database User: autosys (grayed out). The password of the database user.	Typical or Custom	
Secondary Event Server Properties **Note:** This page is displayed only if you selected the Employ Dual Event Servers check box on the CA Workload Automation Database Properties page. The secondary event server settings: ■ Whether you want to create the CA Workload Automation AE database. This check box is selected by default. ■ The logical name of the database server. ■ The name of the database. ■ Whether you want to use Windows authentication. This option is selected by default. ■ Whether you want to use SQL Server authentication. If you select this option, you must specify the SA user name and password.	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: ■ Whether you want to create the database (if the CA Workload Automation AE database does not exist) or refresh the database (if the CA Workload Automation AE database is already installed). This check box is selected by default. If you clear this check box, the installer does not create the database or the tablespaces. ■ The name of the Oracle service. ■ The name of the Oracle SA user. ■ The password of the Oracle SA user.	Typical or Custom	
Primary Event Server Properties AEDB Administrator: aedbadmin (grayed out). The password of the database administrator user.	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
Primary Event Server Properties The event server settings: ■ Whether you want to create the database tablespaces. This check box is selected by default. If you clear this check box, you must create the database tablespaces manually. ■ 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. **Note:** The Using Oracle Managed Files (OMF) option is available only if OMF is enabled on the Oracle server. ■ The name of the tablespace on the event server that contains the database tables. The default name is AEDB_DATA. ■ The database tablespace size. The minimum size is 800 MB. ■ The directory where you want to create the data tablespace. This directory must already be defined on the Oracle server. ■ The name of the tablespace on the event server that contains the database indexes. The default name is AEDB_INDEX. ■ The index tablespace size. The minimum size is 80 MB. ■ The directory where you want to create the index tablespace. This directory must already be defined on the Oracle server.	Typical or Custom	
Primary Event Server Properties CA WAAE Database User: autosys (grayed out). The password of the database user.	Typical or Custom	
Secondary Event Server Properties **Note:** This page is displayed only if you selected the Employ Dual Event Servers check box on the CA Workload Automation Database Properties page. The secondary event server settings: ■ Whether you want to create the database (if the CA Workload Automation AE database does not exist) or refresh the database (if the CA Workload Automation AE database is already installed). This check box is selected by default. If you clear this check box, the installer does not create the database or the tablespaces. ■ The name of the Oracle service. ■ The name of the Oracle SA user. ■ The password of the Oracle SA user.	Custom	

Information Requested	Installation Type	Your Selection or Value
Secondary Event Server Properties AEDB Administrator: aedbadmin (grayed out). The password of the database administrator user.	Custom	
Secondary Event Server Properties The secondary event server settings: ■ Whether you want to create the database tablespaces. This check box is selected by default. If you clear this check box, you must create the database tablespaces manually. ■ 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. **Note:** The Using Oracle Managed Files (OMF) option is available only if OMF is enabled on the Oracle server. ■ The name of the tablespace on the event server that contains the database tables. The default name is AEDB_DATA. ■ The database tablespace size. The minimum size is 800 MB. ■ The directory where you want to create the data tablespace. This directory must already be defined on the Oracle server. ■ The name of the tablespace on the event server that contains the database indexes. The default name is AEDB_INDEX. ■ The index tablespace size. The minimum size is 80 MB. ■ The directory where you want to create the index tablespace. This directory must already be defined on the Oracle server.		

Information Requested	Installation Type	Your Selection or Value
Sybase Only		
Primary Event Server Properties The event server settings: ■ Whether you want to create the database (if the CA Workload Automation AE database does not exist) or refresh the database (if the CA Workload Automation AE database is already installed). 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. ■ The name of the Sybase server where you want to install the database for the primary event server. ■ The name of the database on the Sybase server. The default database name is AEDB. ■ The name of the Sybase SA user. ■ The password of the Sybase SA user.	Typical or Custom	
Primary Event Server Properties The event server settings: ■ 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. ■ Whether you want to use a separate Sybase data device or log device. This check box is selected by default. ■ The name and size of the data device. The default name is AEDB_DATA. The device size must be specified in megabytes. The minimum size is 800 MB. ■ The directory where you want to create the Sybase data device. This directory must exist on the Sybase server. ■ The name and size of the log device. The default name is AEDB_LOG. The device size must be specified in megabytes. The minimum size is 100 MB. ■ The directory where you want to create the Sybase log device. This directory must exist on the Sybase server.	Typical or Custom	
Primary Event Server Properties CA WAAE Database User: autosys (grayed out). The password of the database user.	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 CA Workload Automation Database Properties page. The secondary event server settings: ■ Whether you want to create the database (if the CA Workload Automation AE database does not exist) or refresh the database (if the CA Workload Automation AE database is already installed). 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. ■ 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 name of the Sybase SA user. ■ The password of the Sybase SA user.	Custom	
Secondary Event Server Properties The secondary event server settings: ■ 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. ■ Whether you want to use a separate Sybase data device or log device. This check box is selected by default. ■ The name and size of the data device. The default name is AEDB_DATA. The device size must be specified in megabytes. The minimum size is 800 MB. ■ The directory where you want to create the Sybase data device. This directory must exist on the Sybase server. ■ The name and size of the log device. The default name is AEDB_LOG. The device size must be specified in megabytes. The minimum size is 100 MB. ■ The directory where you want to create the Sybase log device. This directory must exist on the Sybase server.	Custom	
End of database-specific pages.		

Information Requested	Installation Type	Your Selection or Value
Scheduler Properties The scheduler auxiliary listening port. The default 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 check this 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. ■ The Legacy Agent Instance Wide Logging Directory. You can browse and select a different Legacy Agent Instance Wide Logging Directory.	Custom	
High Availability **Note:** This page is displayed only if you selected the Configure High Availability check box on the Scheduler Properties page. The machine function for high availability. You can set the machine to function as a Primary Machine, Shadow Machine, or Tie-Breaker Machine.	Custom	
Database Test Whether the database connection is valid. You must click Start Test to perform a validation on your database connection to proceed.	Typical or Custom	
Program Folder The program folder to which the setup adds program icons.	Custom	
Installation Complete Whether you want to restart your computer to complete the installation. **Note:** This option is displayed if the installation fails to change any SSA related binaries or libraries. This happens if SSA or any other application using SSA is active during the installation.	Typical or Custom	

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

More information:

Host Machine Checklist (see page 47)
Install the Server (see page 70)

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 DVD 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 a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.
3. Run setup.exe.

   The Product Explorer appears.
4. Select CA Workload Automation AE, and click Install.

   The Installation Wizard Welcome page appears.
5. Click Next.

   The License Agreement page appears.
6. Read the license text. When you have scrolled to the bottom of the license text, the I accept the terms of the License Agreement option is enabled. If you agree with the license agreement, select the I accept the terms of the License Agreement option, and click Next.

   Notes:

   - If you select I do NOT accept the terms of the License Agreement option, you cannot continue with the installation. You must select I accept the terms of the License Agreement option or click Cancel.
   - The Detected Software page appears only if the installation wizard finds any installed component of CA Workload Automation AE or CA AC on the computer. You must remove the unwanted components using the Add or Remove Programs on Windows.

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

   The Installation Definition page appears.
8. Select Server and click Next.

   The Installation Type page appears.

9. 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.

10. 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 Setup Status page appears. When the installation completes, the Installation Complete page appears.

    Note: If you want to view the readme, you must select the View the CA Workload Automation Readme File check box on the Installation Complete page. The readme includes information about the known issues in this release.

11. Click Finish.

    The server installation is complete.

More information:

Installation Considerations (see page 56)
Installing the Server, Client, or Agent Silently (see page 129)

Define the Agent on the Server

To enable communication between CA Workload Automation AE and the agent, you must define the agent (see page 97) 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.

How to Verify the Server Installation

Before continuing with the post-installation procedures that may include creating additional EDIT and EXEC superusers, 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 72).
2. Stop the scheduler (see page 72).

3. Start the scheduler (see page 73).
4. Verify the execution of a test job. To do this, do the following:
   - Start the application server (see page 73).
   - Verify that the agent is working and the database is accessible (see page 74).
   - Run a test job (see page 79).

Set the Time Zone

Before you start the scheduler, make sure that the correct time zone is specified in the Control Panel, Date/Time dialog. 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.

Stop the Scheduler

To stop the scheduler, enter the following command:

```
sendevent -E STOP_DEMON
```

This command enables the scheduler to complete any processing before it shuts down.

Notes:

- You must be an EXEC superuser to issue commands and stop the scheduler.
- After you stop the scheduler, you must verify its status using the Services - CA Workload Automation AE Administrator window of CA Workload Automation AE administrator, or from the Services dialog in the Control Panel. For more information about verifying the status of a service using the CA Workload Automation AE Administrator, see the *Online Help*.

More information:

Define Additional EDIT and EXEC Superusers (see page 134)

Start the Scheduler

You must start the scheduler manually using the CA Workload Automation AE Administrator, or from the Services dialog in the Control Panel.

To start the scheduler using CA Workload Automation AE Administrator

1. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select an instance from the Instance drop-down list.
3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the scheduler service, and click Start.

   The scheduler starts. The Status column indicates the status.

Note: You can also use the autosyslog -e command at a CA Workload Automation AE instance command prompt to monitor messages from the scheduler. To stop the log command, press Ctrl+C on your keyboard.

More information:

Start the Scheduler (see page 262)

Start the Application Server

You must start the application server manually using the Services - CA Workload Automation AE Administrator window, or from the Services dialog in the Control Panel.

To start the application server using CA Workload Automation AE Administrator

1. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select an instance from the Instance drop-down list.
3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the application server service, and click Start.

   The application server starts. The Status column indicates the status.

Verifying the Agent and Database Accessibility

You can test the product installation by doing the following:

- Verify the agent accessibility.
- Verify that the database is running.
- Verify the environment and configuration.

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 97) 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 agent accessibility

1. Open the instance command prompt window from the program group.
2. Run the autoping command. For example, if the computer's name is jupiter, enter the following:

   ```
   autoping -m jupiter
   ```

   You must get the following message:

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

   If you do not get the success message in the instance command prompt window, the agent is not configured properly, or it is not started. As a result, CA Workload Automation AE cannot start jobs on that computer (even if it is the same computer as the event server).

Note: You must run commands from an instance command prompt (located in the CA Workload Automation AE program group) because it sets several environment variables required to run the commands.

Verify the Database is Running

You can verify that a database (event server) is running by following the procedure for your database type.

Verify a Microsoft SQL Server Database is Running

You can check the running status of a Microsoft SQL Server database.

To check the running status of a Microsoft SQL Server database

1. Open the IS graphical query interface (located in your Microsoft SQL Server program group). If you are using Microsoft SQL 2005, you can use sqlcmd or OSQL to accomplish the same task.
2. Log on to the server using the autosys user and password. The default password is autosys, but you can change it using the autosys_secure command.
3. If you cannot log on to the server using the ISQL/w interface, check the following:
   a. Log on to a configured computer with the event server and use the Microsoft SQL Service Manager interface to verify that the service is running or to start the service if it is not running.
   b. On the client computers, use the CA Workload Automation AE Administrator to make sure that the parameters on the Event Server - CA Workload Automation AE Administrator window are the same as those entered for the Microsoft SQL Server.

   Note: If the problem still exists, contact your database administrator.

Verify an Oracle Database is Running

You can check the running status of an Oracle database.

To check the running status of an Oracle database

1. Enter the following command at a CA Workload Automation AE instance command prompt:

   ```
   sqlplus User_Name/Password@TNS_Alias
   ```

   User_Name

   Defines your user name.

   Password

   Defines your password.

   TNS_Alias

   Defines your TNS database name.

   The following prompt is displayed:

   ```
   sql>
   ```

2. If you do not get the SQL prompt in the instance command prompt window, follow these steps:

   a. Log on to the configured computer with the event server and verify that SQL*Plus works from there. If the event server is running and accessible on that computer, CA Workload Automation AE was not installed properly on the client computer. In particular, one of the following parameters was probably entered incorrectly: event server name, port number, database name, or event server host.

   b. On the client computer, use the CA Workload Automation AE Administrator to make sure that everything was entered correctly. You can locate the parameter information on the Event Server - CA Workload Automation AE Administrator window.

   Note: If the problem still exists, contact your database administrator.

3. Enter exit.

   You exit SQL*Plus.

Verify a Sybase Database is Running

You can check the running status of a Sybase database.

To check the running status of a Sybase database

1. Enter the following command at a CA Workload Automation AE instance command prompt:

   ```
   isql –Uautosys –Pautosys -SServer_Name -DDatabase_Name
   ```

   -U*autosys*

   Defines your user name.

   -P*autosys*

   Defines your user password.

   -SServer_Name

   Defines your server name.

   -D*Database_Name*

   Defines your database name.

   The following prompt is displayed:

   ```
   1>
   ```

2. If you do not get the SQL prompt, follow these steps:

   a. Log on to a configured computer with the event server and verify that the ISQL utility works from there. If the event server is running and accessible on that computer, CA Workload Automation AE was not installed properly on the client computer. In particular, one of the following parameters was probably entered incorrectly: event server name, port number, database name, or event server host.

   b. Use the CA Workload Automation AE Administrator on the client computer to make sure that all information was entered correctly. You can locate the parameter information on the Event Server - CA Workload Automation AE Administrator window.

   Note: For additional debugging techniques, see the *User Guide* For assistance, contact Technical Support at http://ca.com/support.

3. Enter exit.

   You exit ISQL.

Verify the Environment and Configuration

You must verify the connection to the event server, which is based on the setting of the environment variables (at this point, the database should be running).

To verify the connection to the event server from a CA Workload Automation AE instance command prompt, enter the following command:

```
chk_auto_up
```

You must see a message similar to this, which indicates success:

```
CAUAJM_I_50054 Attempting (1) to Connect with Database: machine:AEDB
CAUAJM_I_50055 *** Have Connected successfully with Database: machine:AEDB. ***
______________________________________________________________________________

CAUAJM_I_50128 Connected with Event Server: machine:AEDB


______________________________________________________________________________


______________________________________________________________________________

CAUAJM_I_50038 Checking CA WAAE Scheduler on Machine: machine
CAUAJM_I_50044 Primary Scheduler is RUNNING on machine: machine
______________________________________________________________________________
```

The chk_auto_up command also lets you check whether the event servers and the schedulers are running.

You must run commands from the instance command prompt (located in the CA Workload Automation AE program group) because it sets several environment variables required to run the commands. If you used this command prompt and did not get the previous message, some diagnostic messages that contain information about the problem are displayed.

Note: For more information about the chk_auto_up command, see the *Reference 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 or GUI programs, first verify that CA Workload Automation AE has been enabled using the AutoSys 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. You can also define jobs using the Job Editor, which you can open from your CA Workload Automation AE program group.

A test job named test_install is included with the product. Its job definition is in the file named %AUTOSYS%\test\jil\test_install. Use the test_install job as a template to verify the installation.

Specify a Computer Name in the test_install Job

If 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. Log in as the user whose user ID and password you entered following the steps in Adding the Superusers and the Windows User IDs and Passwords (see page 133).

   Note: The user who defines the job and is the owner of the job must be a valid user on the computer on which you want to run the job.

2. Edit the test_install script by using the following command:

   ```
   notepad %AUTOSYS%\test\jil\test_install
   ```

3. Replace NT_HOSTNAME in the computer: NT_HOSTNAME line with the host name of the Windows computer you are currently logged on to. For example, if the host name is called sales, you must enter the following:

   ```
   insert_machine: sales
   ```

   Note: The NT_HOSTNAME computer must be defined using jil, otherwise the job is not inserted.

4. Save the test_install script and enter the following command at the instance command prompt:

   ```
   jil < %AUTOSYS%\test\jil\test_install
   ```

   The machine (sales) is inserted into the database. The output is similar to the following:

   ```
   Insert/Updating Machine: "sales"
   Database Change was Successful!
   ```

5. Delete the following line from the %AUTOSYS%\test\jil\test_install script, and save and close the file:

   ```
   insert_machine: sales
   ```

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!
```

Note: If c:\tmp directory does not exist, create it so that the job can write the files to this directory.

Run the Test Job

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

```
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.

More information:

Adding the Superusers and the Windows User IDs and Passwords (see page 133)

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.

If you see an error message in the scheduler output log that indicates it was unable to log you on as user@domain, you either entered an incorrect password or entered a password for a user other than the job owner. You can identify the job owner by running the following command at the instance command prompt:

```
autorep -J test_install -q
```

You can verify that you entered this specific user ID and password with the autosys_secure command for the job owner. If it is necessary, you can use the autosys_secure command to enter the correct user logon ID and password.

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, 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.

More information:

How to Install the Client (see page 84)
Installation Checklist for the CA Workload Automation AE Client (see page 85)

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 71).
2. Collect the required information (see page 85).

   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 87).
4. Define the agent on CA Workload Automation AE (see page 89).
5. Verify the installation (see page 89).

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 46) 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 Type The type of installation to perform: ■ Typical ■ Custom	Typical or Custom	
Installation Definition The definition of the installation to perform: ■ Server ■ Client ■ Agent	Typical or Custom	

Information Requested	Installation Type	Your Selection or Value
Installation Path The preferred installation drive. The CA Workload Automation AE installation path. The default installation path is C:\Program Files\CA\Workload Automation AE. The CA Shared Directory installation path. The default installation path is C:\Program Files\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 to encrypt data using the default or a user-specified key. The Encrypt data using Workload Automation default encryption key option is selected by default. If you select Encrypt the data using a user-specified 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 Properties 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.	Typical or Custom	
Program Folder The program folder to which the setup adds program icons.	Custom	
Installation Complete Whether you want to restart your computer to complete the installation. **Note:** This option is displayed if the installation fails to change any SSA related binaries or libraries. This happens if SSA or any other application using SSA is active during the installation.	Typical or Custom	

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

More information:

Host Machine Checklist (see page 47)
Install the Client (see page 87)

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 DVD 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 a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.
3. Run setup.exe.

   The Product Explorer appears.
4. Select CA Workload Automation AE, and click Install.

   The Installation Wizard Welcome page appears.
5. Click Next.

   The License Agreement page appears.

6. Read the license text. When you have scrolled to the bottom of the license text, the I accept the terms of the License Agreement option is enabled. If you agree with the license agreement, select the I accept the terms of the License Agreement option, and click Next.

   Notes:

   - If you select I do NOT accept the terms of the License Agreement option, you cannot continue with the installation. You must select I accept the terms of the License Agreement option or click Cancel.
   - The Detected Software page appears only if the installation wizard finds any installed component of CA Workload Automation AE or CA AC on the computer. You must remove the unwanted components using the Add or Remove Programs on Windows.

   The Installation Function page appears.

7. Select New and click Next.

   The Installation Definition page appears.

8. Select Client and click Next.

   The Installation Type page appears.

9. 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.

10. 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 Setup Status 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 select the View the CA Workload Automation Readme File check box on the Installation Complete page. The readme includes information about the known issues in this release.

11. Click Finish.

    The client installation is complete.

More information:

Installation Considerations (see page 83)
Installing the Server, Client, or Agent Silently (see page 129)

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 97) 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.

Verify the Client Installation

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.

Note: After you install the agent, you must define that agent on CA Workload Automation AE (see page 97) 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.

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.

You can install the agent in the following ways:

- 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 as follows:
  - By selecting the Additional CA Workload Automation Agent option on the CA Workload Automation AE 11.3 Product Explorer window. This option lets you install the agent on remote computers or to install multiple agents on a single computer.
  - By selecting the Register packages to Unicenter SD for Windows option on the CA Workload Automation AE 11.3 Product Explorer window. This option lets you register the agent with CA SDM on your computer so that you can use CA SDM to install additional agents.

More Information:

Install Multiple Agents on a Single Computer (see page 103)
Install Additional Agents Using CA SDM (see page 104)

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 92).

   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. Install the agent (see page 95).
4. Define the agent on CA Workload Automation AE (see page 97).
5. Verify the installation (see page 100).
6. (Optional) Modify the agent configuration settings (see page 143).

Installation Checklist for the CA Workload Automation AE 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 46) installed during a typical agent installation are as follows:

- Agent
- CA Secure Socket Adapter (SSA)

Information Requested	Installation Type	Your Selection or Value
Installation Type The type of installation to perform: ■ Typical ■ Custom	Typical or Custom	
Installation Definition The definition of the installation to perform: ■ Server ■ Client ■ Agent	Typical or Custom	
Installation Path The preferred installation drive. The CA Workload Automation AE installation path. The default installation path is C:\Program Files\CA\Workload Automation AE. The CA Shared Directory installation path. The default installation path is C:\Program Files\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	
Data Encryption The type of data encryption. You can select to encrypt data using the default or a user-specified key. The Encrypt data using Workload Automation default encryption key option is selected by default. If you select Encrypt the data using a user-specified 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 ServerPorts 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.	Custom	
Agent Information The agent name. The default agent name is WA_AGENT. The agent port number. The default port number is 7520. If port multiplexing is selected, the default port number is 49154. The agent settings: ■ 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.	Typical or 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	
Program Folder The program folder to which the setup adds program icons.	Custom	
Installation Complete Whether you want to restart your computer to complete the installation. **Note:** This option is displayed if the installation fails to change any SSA related binaries or libraries. This happens if SSA or any other application using SSA is active during the installation.	Typical or Custom	

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

More information:

Host Machine Checklist (see page 47)
Install the Agent (see page 95)

Install the Agent

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:

- If you have installed the CA Workload Automation AE server or client on this computer, the agent is already installed.
- You can install the agent using the CA Workload Automation AE DVD 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 agent

1. Log in as a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.
3. Run setup.exe.

   The Product Explorer appears.
4. Select CA Workload Automation AE, and click Install.

   The Installation Wizard Welcome page appears.
5. Click Next.

   The License Agreement page appears.

6. Read the license text. When you have scrolled to the bottom of the license text, the I accept the terms of the License Agreement option is enabled. If you agree with the license agreement, select the I accept the terms of the License Agreement option, and click Next.

   Notes:

   - If you select I do NOT accept the terms of the License Agreement option, you cannot continue with the installation. You must select I accept the terms of the License Agreement option or click Cancel.
   - The Detected Software page appears only if the installation wizard finds any installed component of CA Workload Automation AE or CA AC on the computer. You must remove the unwanted components using the Add or Remove Programs on Windows.

   The Installation Function page appears.

7. Select New and click Next.

   The Installation Definition page appears.

8. Select Agent and click Next.

   The Installation Type page appears.

9. 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.

10. 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 Setup Status 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 select the View the CA Workload Automation Readme File check box on the Installation Complete page. The readme includes information about the known issues in this release.

11. Click Finish.

    The agent installation is complete.

More information:

Installing the Server, Client, or Agent Silently (see page 129)

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter **jil** at the instance command 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
```

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. Test communication between CA Workload Automation AE and the agent (see page 100).
2. Define a test job (see page 101).
3. Run the test job (see page 102).
4. Monitor the test job (see page 102).

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter the following command at the instance command 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 Windows script, to test communication between CA Workload Automation AE and the agent.

To define a test job

1. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter **jil** at the instance command 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: "C:\sleep.exe" 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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter the following commands at the instance command 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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter the following commands at the instance command 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 a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.
3. Run setup.exe.

   The Product Explorer appears.
4. Select Additional CA Workload Automation Agent, and click Install.

   The Application Server Ports page appears.
5. Enter the application server port number in the Port Numbers(s) field, and click Next.

   Note: If the agent must communicate with multiple application servers that are configured to use a port other than the default (9000), you must enter multiple ports by separating each port number with a comma.

   The Agent Information page appears.
6. Complete the fields as appropriate, and click Next.

   The Review Settings page appears.

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 Setup Status page appears and the progress is displayed. When the installation completes, the Installation Complete page appears.

8. Click Finish.

   The agent installation is complete.

Install Additional Agents Using CA SDM

You can also install additional agents by registering the agent with CA SDM on your computer. After the agent is registered with CA SDM, you can use CA SDM to install additional agents.

Note: For more information about setting up CA Workload Automation AE to be delivered through CA SDM, see the Software Distribution Manager documentation.

To install additional agents using CA SDM

1. Log in as a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.

3. Run setup.exe.

   The Product Explorer appears.

4. Select Register packages to Unicenter SD for Windows, and click Install.

   The Choose Products to Register page appears. By default, the CA Workload Automation AE Agent 11.3 check box is selected.

5. Click Next.

   The Unicenter Software Delivery User Details page appears.

6. Complete the fields as appropriate, and click Next.

   The Registering Products page appears and the progress is displayed. When the registration is complete, the Complete button is enabled.

7. Click Complete.

   The registration is complete. You can now install additional agents using CA SDM.

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. Open the CA Workload Automation AE Product Explorer.
2. Expand the Silent Installs folder.
3. Select Response File Generation Installation Wizard.
4. Click Install.

   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

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

   ```
   setup.exe –S –f1 Response_file_path
   ```

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

6. (For Oracle only) Create an oracle instance using dbca.

7. (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.

8. Create a directory to store the database creation log.

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

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

   - For Microsoft SQL Server: %AUTOSYS%\dbobj\MSSQL
   - For Oracle: %AUTOSYS%\dbobj\ORA
   - For Sybase: %AUTOSYS%\dbobj\SYB

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

    - Run the CreateAEDB script in console mode.
    - Run the CreateAEDB script in interactive mode: for Microsoft SQL Server (see page 111), for Oracle (see page 113) or for Sybase.

    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\MSQ\CreateAEDB.pl (for Microsoft SQL Server)
- %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 Microsoft SQL Server

```
perl CreateAEDB.pl "ADB_DATASERVER" "ADB_DATABASE" "ADB_SA_USER" "ADB_SA_PSWD"
"ADB_WA_DB_PSWD" "JAVA_HOME" "ADB_OUTDIR" "CREATE_DB" "ADB_DEBUG"
```

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 Microsoft SQL Server or Sybase database name.

ADB_DATASERVER

- Microsoft SQL Server—Specifies the machine name where the Microsoft SQL server is running.
- Sybase—Specifies the Sybase server name, as defined in the %SYBASE%\ini\sql.ini 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 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.

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 Microsoft SQl Server, Oracle, or Sybase ‘autosys’ user password. If the autosys user is already defined in Microsoft SQL Server, Oracle or Sybase, you must specify the valid password. If the autosys user is not defined, 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 a Database on Microsoft SQL Server

This example creates a Microsoft SQL Server database named AEDB on server LAM04.

```
perl CreateAEDB.pl “LAM04” “AEDB” “sa” "sapassword" “autosyspw”
“C:\Progra~1\CA\SC\JRE\1.5.0_11” “C:\tmp\adblog” “Y” "N"
```

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"
"D:\Program Files\CA\SC\JRE\1.5.0_11" “\tmp\adblog” "Y" "AEDB_DATA"
"\home\oracle\oradata" "800" "AEDB_INDEX" "C:\oracle\oradata\SERVER_NAME" "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” “D:\Program
Files\CA\SC\JRE\1.5.0_11” “\tmp\adblog” “Y” "AEDB_DATA" "\opt\sybase\data" "800"
"AEDB_LOG" "%SYBASE%\data" "80" "N"
```

Run the CreateAEDB Script for Microsoft SQL Server in Interactive Mode

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

To run the CreateAEDB script for Microsoft SQL Server in interactive mode

1. Make sure the MSSQL bin path is in System PATH, and then issue the following commands:

   ```
   cd %AUTOSYS%\dbobj\MSQ
   perl CreateAEDB.pl
   ```

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

   Server name?

   Enter the Microsoft SQL Server server name.

   Default: HOSTNAME

   Database name?

   Enter the name you want the Microsoft SQL Server database to be called.

   Default: AEDB

   User name with system admin privileges?

   Enter the Microsoft SQL Server system administrator user ID.

   Default: sa

   sa user's password?

   Enter the Microsoft SQL Server system administrator user password.

   Default: sa

   Note: When you press Enter to accept the password, CreateAEDB verifies that it can connect to Microsoft SQL Server. 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 Microsoft SQL Server ‘autosys’ user password.

   Default: autosys

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

   JRE Directory?

   Enter the JAVA_HOME path.

Default: %CASHCOMP%\JRE\1.5.0_11

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

   Create a new DB? (Y|N)

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

   Default: N

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 Microsoft SQL Server if you chose to create the database. Otherwise, the database is refreshed.

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: D:\Program Files\CA\SC\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: D:\Program Files\CA\SC\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 [**%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: %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\MSQ\RefreshAEDB.pl (for Microsoft SQL Server)
- %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 Microsoft SQL Server

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

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 a Database on Microsoft SQL Server

This example updates a Microsoft SQL Server database named AEDB on server LAM04.

```
perl RefreshAEDB.pl "LAM04" "AEDB" "sa" "sapassword" "autosyspw"
"C:\Progra~1\CA\SC\JRE\1.5.0_11" "C:\tmp\adblog" "Y" "N"
```

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" "D:\Program Files\CA\SC\JRE\1.5.0_11"
“C:\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" "D:\Program
Files\CA\SC\JRE\1.5.0_11" "C:\tmp\adblog" "N"
```

Run the RefreshAEDB Script for Microsoft SQL Server in Interactive Mode

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

To run the RefreshAEDB script for MSSQL in interactive mode

1. Make sure MSSQL osql is in PATH, and then issue the following commands:

   ```
   cd %AUTOSYS%\dbobj\MSQ
   perl RefreshAEDB.pl
   ```

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

   Server name?

   Enter the MSSQL server name.

   Default: Hostname

   Database name?

   Enter the MSSQL database to be called.

   Default: AEDB

   User name with system admin privileges?

   Enter the MSSQL system administrator user ID.

   Default: sa

   sa user's password?

   Enter the MSSQL system administrator user password.

   Default: sa

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

   ```
   The host,/userid/password combination is valid.
   ```

   JRE Directory?

   Enter the JAVA_HOME path.

   Default: D:\Program Files\CA\SC\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 MSSQL.

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: D:\Program Files\CA\SC\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: D:\Program Files\CA\SC\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:

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.

Install the SDK Runtime Environment

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

1. Open the CA Workload Automation AE Product Explorer.
2. Expand the Standalone Installs folder.
3. Select CA Workload Automation AE SDK.
4. Click Install.

   The CA Workload Automation AE installation wizard appears.
5. Click Next.

   The License Agreement page appears.
6. 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.

7. Choose the installation directory of the CA product that must communicate with CA Workload Automation AE, and click Next.

   The Review Settings page appears, listing the default settings.

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

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

9. Click Finish.

   You are prompted to reboot. The SDK runtime environment is installed.

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. Open the CA Workload Automation AE Product Explorer.
2. Expand the Standalone Installs folder.
3. Select CA Workload Automation AE SDK.
4. Click Install.

   The CA Workload Automation AE installation wizard appears.

5. Click Next.

   The Installation Path page appears.

6. Click Next.

   The Review Settings page appears, listing the default settings.

7. Click Next.

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

8. Click Finish.

   The reinstallation is complete.

Remove the SDK Runtime Environment

If you no longer need the SDK runtime environment, you can remove it using Windows Add or Remove Programs.

To remove the SDK runtime environment

1. Open Add or Remove Programs from the Windows Control Panel.
2. Select CA Workload Automation AE and select Uninstall.

   The Product Removal Selection page appears.
3. Click Next.
4. Follow the prompts to complete the uninstall.

   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 130).
2. Install the server, client, or agent silently (see page 131).

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.

Notes:

- The server, client, or agent will not be installed when you are creating the response file.
- Alternatively, you can run the installation in record mode using the Response File Generation installation wizard located in the Product Explorer.

To create a response file

1. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.

2. Close all windows, except a command prompt.
3. Change directories to your DVD drive and go to your %AutoSys% directory as follows:

   ```
   cd /d DVD_drive:
   ```

   DVD_drive

   Identifies the installation media drive.

4. Run the following command:

   ```
   setup.exe /r /f1”directory_path\response_file.iss”
   ```

   directory_path

   Specifies the path where the response file should be created.

   response_file

   Defines the name of the response file.

   Note: There cannot be a space between the /f1 option and the double quotes preceding the directory path; if there is a space, the installation fails.

   The Welcome page appears.

5. Click Next.

   The License Agreement page appears.

6. Read the license text. When you have scrolled to the bottom of the license text, the I accept the terms of the License Agreement option is enabled. If you agree with the license agreement, select the I accept the terms of the License Agreement option, and click Next.

   Note: If you select I do NOT accept the terms of the License Agreement option, you cannot continue with the installation. You must select I accept the terms of the License Agreement option or click Cancel.

   The Installation Type page appears.

7. 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.

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.

   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 at installation time. Instead, silent installation uses your previously-created response file to provide the required information.

To install the server, client, or agent silently

1. Copy the response file to the specified directory path on the computer on which you want to run the silent installation.

2. Run the following command in a command prompt from the installation media drive:

   ```
   setup.exe /s /f1”directory_path\response_file.iss”
   ```

   directory_path

   Specifies the path where the response file was copied.

   response_file

   Specifies the name of an existing response file.

   Note: There cannot be a space between the /f1 option and the double quotes preceding the directory path; if there is a space, the installation fails.

   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:

Adding the Superusers and the Windows User IDs and Passwords

When an Agent runs a job, the Agent logs on to the remote computer as the owner of the job. To do this, the Agent uses the encrypted passwords that were passed to it with the job request by the scheduler. The scheduler gets these passwords from the event server (database). Therefore, after the installation is complete and before you can run jobs, you must enter Windows user IDs and passwords for users who define and run jobs.

Before you can enter the Windows user IDs and passwords in the database, you must first establish the 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.

Note: For information about the logon procedures used, see the *User Guide*. For information about job ownership, see the *Reference Guide*.

Define Additional EDIT and EXEC Superusers

After installation, you can define additional EDIT and EXEC superusers.

To define the EDIT and EXEC superusers

1. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter the following command at the instance command 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
   ```

3. Enter 2 and press the Enter key.

   The manage EDIT/EXEC superuser 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.
- Be sure to run all commands at a CA Workload Automation AE instance command prompt located in the CA Workload Automation AE program group. The instance command prompt windows set several environment variables that are required to run commands.
- For more information about the autosys_secure command, see the *Reference Guide*.

Add the Windows User IDs and Passwords

Before you can run jobs on Windows, you must enter the Windows user IDs and passwords for all users on all domains who define and run jobs. We recommend that you add only the user and password needed to run a test job before adding other users. After you have successfully created and run the test job, you can add additional Windows user IDs and passwords.

To add a Windows user ID and password to the database

1. Log in to Windows as the EDIT superuser.
2. Open a CA Workload Automation AE instance command prompt window from your program group.
3. Enter the following command at the instance command 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
   ```

4. Enter 5 and press the Enter key.

   The manage user@host users menu is displayed.

5. Enter 1 and press the Enter key.

   The create user@host or domain password menu is displayed.

6. Enter the user name, host or domain name, new password, and password confirmation.

   Note: Windows user IDs must not exceed 20 characters, and they can include any characters except the following:

   " / ; : < > | = + *

   Windows passwords are case-sensitive and must not exceed 14 characters, and they can contain any character except a space.

   If the user is created successfully, the user information is entered into the database with the encrypted password.

Note: For more information about creating, changing, and deleting user IDs and passwords, see the *Reference Guide*.

More information:

Running a Test Job (see page 79)

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
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:

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 a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.
3. Run setup.exe.

   The Product Explorer appears.
4. Select CA Workload Automation AE, and click Install.

   The Installation Wizard Welcome page appears.
5. Select Modify and click Next.

   The Modify Installation Function page appears.
6. Select Add Features and click Next.

   The Installed Instances page appears.
7. Select the instance you want to add features to, and click Next.

   The Components page appears.
8. Select the additional features you want to install, and click Next.

9. 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.

10. 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 a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.

3. Run setup.exe.

   The Product Explorer appears.

4. Select CA Workload Automation AE and click Install.

   The Installation Wizard Welcome page appears.

5. Select Modify and click Next.

   The Modify Installation Function page appears.

6. Select Add Instance and click Next.

   The Instance Information page appears.

7. Enter a name for the new instance and click Next.

   The Installation Function page appears.

8. 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.

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 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 a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.

3. Run setup.exe.

   The Product Explorer appears.

4. Select CA Workload Automation AE, and click Install.

   The Installation Wizard Welcome page appears.

5. Select Modify and click Next.

   The Modify Installation Function page appears.

6. Select Delete Instance and click Next.

   The Installed Instances page appears.

7. Select the instance to delete and click Next.

   The Review Settings page appears, listing the instance name you selected.

8. 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.

Repair an Existing CA Workload Automation AE Installation

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 repair an existing installation

1. Make sure all CA Workload Automation AE components are closed.
2. Log in as a user with Windows Administrators group privileges.
3. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.
4. Run setup.exe.

   The Product Explorer appears.
5. Select CA Workload Automation AE, and click Install.

   The Installation Wizard Welcome page appears.
6. Select Repair and click Next.

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

   The Setup Status page appears and the progress is displayed. When the update completes, the Installation Complete page appears.
8. Click Finish.

   The reinstallation is complete.

More Information:

Post-Installation Procedures for the Server (see page 133)

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 151)

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 97)
2. Define a user on CA Workload Automation AE (see page 146).
3. Setting up security permissions on CA Workload Automation AE (see page 147).
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 100).

More Information:

Agents and Agent Plug-ins (see page 17)

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:

- 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 enter the following command at the instance command 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.
   ```

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 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 97)
Define a User on CA Workload Automation AE (see page 146)

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. Do the following:

   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the agent service, and click Stop.

      The agent stops.

2. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

3. Enter **jil** at the instance command 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 | <u>DEFAULT</u> | 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.

<u>DEFAULT</u>

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. Do the following:

   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the agent service, and click 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 143)

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. Do the following:

   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the agent service, and click Stop.

      The agent stops.

2. Open the agentparm.txt file located in the agent installation directory.

3. Edit the parameters to make the required changes.

4. Save and close the agentparm.txt file.

5. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

6. Enter **jil** at the instance command 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 | <u>DEFAULT</u> | 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.

<u>DEFAULT</u>

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. Do the following:

    a. Click Start, Programs, CA, Workload Automation AE, Administrator.

       The Instance - CA Workload Automation AE Administrator window opens.

    b. Select your CA Workload Automation AE instance from the Instance drop-down list.

    c. Click the Services icon on the toolbar.

       The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

    d. Right-click the agent service, and click 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 instance command prompt:

```
update_machine: machine1
agent_name: WA_MACH2
```

Note: You must stop and restart the agent for the changes to take effect.

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. Do the following:
   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the agent service, and click Stop.

      The agent stops.

2. Open the agentparm.txt file located in the agent installation directory.

3. Edit or add the communication parameters as appropriate, and save the file.
4. Do the following:
   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.
   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the agent service, and click Start.

      The agent starts.

   The agent 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 159).
2. Define the agent SSA port on CA Workload Automation AE (see page 161).
3. Test communication between CA Workload Automation AE and the agent (see page 100).

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 do the following:
   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.
   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the scheduler, application server, and the agent service, and click Stop.

      The scheduler, application server, and the agent stop.

2. Stop the CA Connection Broker service from the Windows Service Control Manager.
3. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt is displayed.

4. Change to the %CSAM_SOCKADAPTER%\bin folder, and enter the following command:

   ```
   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. Start the CA Connection Broker service from the Windows Service Control Manager.
6. Open the agentparm.txt file located in the agent installation directory.

7. 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_pa
   th/Csam/SockAdapter/bin/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: C:\Program Files\CA\SC

   Note: Append the location of the casocket.jar file to the classpath to specify the location of SSA.

8. Do the following:

   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the scheduler, application server, and the agent service, and click Start.

      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 143)

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt is displayed.

2. Enter **jil** at the instance command 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 172)

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 the Agent on z/OS (see page 172)

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 the Agent on z/OS (see page 172)

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 166)
2. Define a unique communication alias for the application server (see page 168).
3. Set encryption for z/OS communication (see page 170).
4. (AES 128-bit encryption only) Generate an instance-wide communication alias encryption file.
5. Configure the AGENTDEF data set on the agent on z/OS (see page 172).
6. Define the agent on z/OS on CA Workload Automation AE (see page 175).
7. Verify that the agent on z/OS works with CA Workload Automation AE (see page 177).

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. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Click the Scheduler icon on the toolbar.

   The Scheduler - CA Workload Automation AE Administrator window appears.

3. Enter the port number in the Auxiliary Listening Port field in the Communication Ports pane, and click Apply.

   The scheduler auxiliary listening port is defined. The scheduler uses this port to communicate with CA Workload Automation EE and the agent on z/OS. This port is used for all non-SSA communication.

4. Click the Application Server icon on the toolbar.

   The Application Server - CA Workload Automation AE Administrator window appears.

5. Enter the port number in the Communication Alias Identifier field, and click Apply.

   The application server auxiliary listening port is defined. The application server uses this port to communicate with CA Workload Automation EE and the agent on z/OS. This port is used for all non-SSA communication.

6. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

7. Change to the %CSAM_SOCKADAPTER%\bin folder, and enter the following command:

   ```
   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 Auxiliary Listening Port field on the Scheduler - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.

   Port multiplexing and SSL encryption are disabled for the specified scheduler auxiliary listening port.

8. Enter the following command:

   ```
   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 Communication Alias Identifier field on the Application Server - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.

   Port multiplexing and SSL encryption are disabled for the specified application server auxiliary listening port.

9. Do the following:

   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select an instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the scheduler service, and click Stop.

      The scheduler stops.

   e. Right-click the application server service, and click Stop.

      The application server stops.

10. Stop the CA Connection Broker service from the Windows Service Control Manager.

11. Do the following:

    a. Click Start, Programs, CA, Workload Automation AE, Administrator.

       The Instance - CA Workload Automation AE Administrator window opens.

    b. Select an instance from the Instance drop-down list.

    c. Click the Services icon on the toolbar.

       The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

    d. Right-click the scheduler service, and click Start.

       The scheduler starts.

    e. Right-click the application server service, and click Start.

       The application server starts.

    The scheduler and application server auxiliary listening ports are configured.

Note: For more information about the CA Workload Automation AE Administrator, see the *Online Help*.

Define a Unique Communication Alias for an Application Server

The application server requires an additional communication alias to communicate with CA Workload Automation EE and 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.

The default value is *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.

Note: The scheduler also requires a communication alias to communicate with CA Workload Automation EE and 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. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select an instance from the Instance drop-down list.

3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the application server service, and click Stop.

   The application server stops.

5. Click the Application Server icon on the toolbar.

   The Application Server - CA Workload Automation AE Administrator window appears.

6. Enter a unique communication alias in the Communication Alias Identifier field, and click Apply.

   Note: You can enter a maximum of 16 characters (in uppercase). If you specify this value in lowercase or mixed case, it is automatically changed to uppercase.

7. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

8. Right-click the application server service, and click Start.

   The application server starts. The unique communication alias is defined for the application server. The application server uses this alias to communicate with CA Workload Automation EE and the agent on z/OS.

Set Encryption for z/OS Communication

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 clear the Use AES 128-bit encryption when communicating with zOS managers check box.
- 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

1. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select the instance you want to set encryption for from the Instance drop-down list.
3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the scheduler and application server services, and click Stop.

   The scheduler and application server stop.

5. Click the Instance icon on the toolbar.

   The Instance - CA Workload Automation AE Administrator window appears.

6. Click the zOS Encryption tab, and select the Use AES 128-bit encryption when communicating with zOS managers check box.

   The Hexadecimal Key and Verify Hexadecimal Key fields are enabled.

   Note: If you clear the Use AES 128-bit encryption when communicating with zOS managers check box, CA Workload Automation AE uses no encryption for z/OS communication.

7. Enter the encryption key, confirm the encryption key in the Verify Hexadecimal Key field, and click Apply.

   Note: The encryption key must be a hexadecimal string of 32 characters.

   The zOS Encryption Status field displays the current encryption set for the instance.

8. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

9. Right-click the scheduler and application server services, and click Start.

   The scheduler and application server start. The encryption for z/OS communication is set.

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter the following command:

   ```
   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.

AGENTDEF Operand	Description	Corresponding CA Workload Automation AE Setting
COMMCHAN *AutoServerAliasId*	Specifies the name associated with the encryption data between CA Workload Automation AE and the agent on z/OS.	Communication Alias Identifier field on the Application Server - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.
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.	Auxiliary Listening Port field on the Scheduler - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.
PORT(*appsrv_aux_port*)	Specifies the port number that the CA Workload Automation AE application server uses for all non-SSA communication.	Auxiliary Listening Port field on the Application Server - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.
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 162)

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter **jil** at the instance command 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 100)
2. Define a z/OS job (see page 178).
3. Run the test job (see page 102).
4. Monitor the test job (see page 102).

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter **jil** at the instance command 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 183).

Windows Integration Considerations

The following are important considerations when you integrate CA Workload Automation AE with Event Management on Windows:

- The installation sets the Event Manager node as an environmental variable (CA_OPER_NODE) in the Event Agent environment. When this environmental variable is set, all messages that arrive on the Event Agent are sent to that managing node.
- If the CA_OPER_NODE environmental variable is not set, messages that arrive on the Event Agent that must be sent to another node must have a Message Record with a FORWARD action defined in their local message policy file.
- If the Event Manager node changes after installation, you must use the cautenv command to modify the CA_OPER_NODE environmental variable, and stop and start the Event Agent to implement your changes.

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 enter the following command at the instance command prompt:

   ```
   sendevent -E STOP_DEMON
   ```

   The scheduler completes any processing it is currently performing and stops.

2. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

3. Select an instance from the Instance drop-down list.

4. Click the Integration icon on the toolbar.

   The Integration - CA Workload Automation AE Administrator window appears.

5. Select the Forward All CA WAAE Messages check box in the Event Management pane, and click Apply.

   All CA Workload Automation AE messages are forwarded to the Event Management console.

6. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears.

7. Right-click the scheduler service, and click Start.

   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 188)
Configure the Application Server to Listen on a Different Virtual Port (see page 191)

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 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 EXEC superuser and do the following:

   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the scheduler, application server, and the agent service, and click Stop.

      The scheduler, application server, and the agent stop.

2. Stop the CA Connection Broker service from the Windows Service Control Manager.

3. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt is displayed.

4. Change to the %CSAM_SOCKADAPTER%\bin folder, and enter the following command:

   ```
   csamconfigedit Port=value EnableSSL=True EnablePmux=True display
   ```

   Notes:

   - If you defined an application server port using CA Workload Automation AE Administrator, you must use the same port number for Port=*value*. For more information about defining the communication ports for the application server using CA Workload Automation AE Administrator on Windows, see the *Online Help*.

   - 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. Start the CA Connection Broker service from the Windows Service Control Manager.
6. Do the following:
    a. Click Start, Programs, CA, Workload Automation AE, Administrator.

       The Instance - CA Workload Automation AE Administrator window opens.
    b. Select an instance from the Instance drop-down list.
    c. Click the Services icon on the toolbar.

       The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.
    d. Right-click the scheduler, application server, and the agent service, and click Start.

       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.

```
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.

```
csamconfigedit PortRange=49152-50176 ServerStyle=Mandate EnablePmux=True
EnableSSL=True
```

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 do the following:
   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.
   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the scheduler, application server, and the agent service, and click Stop.

      The scheduler, application server, and the agent stop.

2. Stop the CA Connection Broker service from the Windows Service Control Manager.
3. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt is displayed.
4. Change to the %CSAM_SOCKADAPTER%\bin folder, and enter the following command:

   ```
   csamconfigedit Port=value EnablePmux=True
   ```

   value

   Defines the port number to configure.
5. Enter the following command at the instance command prompt:

   ```
   csamconfigedit Port=value display
   ```

   The configuration settings of the specified virtual port are displayed.
6. Start the CA Connection Broker service from the Windows Service Control Manager.
7. Do the following:
   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the scheduler, application server, and the agent service, and click Start.

      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.

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 do the following:
    a. Click Start, Programs, CA, Workload Automation AE, Administrator.

       The Instance - CA Workload Automation AE Administrator window opens.
    b. Select your CA Workload Automation AE instance from the Instance drop-down list.
    c. Click the Services icon on the toolbar.

       The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.
    d. Right-click the scheduler, application server, and the agent service, and click Stop.

       The scheduler, application server, and the agent stop.
2. Stop the CA Connection Broker service from the Windows Service Control Manager.
3. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt is displayed.

4. Change to the %CSAM_SOCKADAPTER%\bin folder, and enter the following command:

   ```
   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. Start the CA Connection Broker service from the Windows Service Control Manager.
6. Do the following:
   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select your CA Workload Automation AE instance from the Instance drop-down list.
   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the scheduler, application server, and the agent service, and click Start.

      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 services and a library. On Windows, the Cross-Platform Interface in CA Workload Automation AE accesses the CAICCI API through the shared library.

On Windows, CAICCI consists of the following four services:

quenetd

Sends or receives messages to or from other Windows hosts and AS/400 hosts.

ccirmtd

Transmits data across the network remotely.

ccinrsd

Defines the name resolution service that provides a unique location where applications may go to make inquires about the location of other applications using CAICCI.

ccinrcd

Defines the name resolution client. It is the client counterpart to the ccinrsd service.

CA Workload Automation AE uses CAICCI to communicate with the following products:

- CA NSM Event Management
- Notification Services component of CA NSM
- CA Workload Automation SE
- CA Workload Automation EE
- CA AutoSys WA Connect Option
- CA Jobtrac JM
- CA Scheduler JM

ccirmtd.rc File—Identify Local and Remote Parameters

The ccirmtd.rc file identifies the local CAICCI node name, the Windows host name, and the block size for the local and remote computers.

The ccirmtd.rc file is located at C:\Program Files\CA\SC\CA_APPSW\ccirmtd.rc or C:\CA_APPSW\ccirmtd.rc.

Note: This path assumes that CA Workload Automation AE is installed on your C drive.

To enable CAICCI communication between computers, you must add the CAICCI REMOTE parameter, so that CAICCI knows how to connect to the nodename and which port to connect to.

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 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 recommend 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.

retry=*x*

(Optional) Determines how the ccirmtd service 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.

port=*p*

(Optional) Specifies another port for this specific connection only.

Default: 1721

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
```

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

Start CAICCI

After you configure CAICCI, you must start CAICCI for the configuration settings to take effect.

Note: You must have administrator privileges to start or stop CAICCI.

To start CAICCI, enter *one* of the following commands:

```
C:\Program Files\CA\SC\CA_APPSW\ccicntrl start
```

or

```
C:\CA_APPSW\ccicntrl start
```

Stop CAICCI

Note: You must have administrator privileges to start or stop CAICCI.

To stop CAICCI, enter *one* of the following commands:

```
C:\Program Files\CA\SC\CA_APPSW\ccicntrl stop
```

or

```
C:\CA_APPSW\ccicntrl stop
```

Check the CAICCI Status

To check the status of CAICCI, enter *one* of the following commands:

```
C:\Program Files\CA\SC\CA_APPSW\ccicntrl status
```

or

```
C:\CA_APPSW\ccicntrl status
```

CAICCI Environment Variables on Windows

On Windows, several CAICCI environment variables are used. These environment variables are usually set as system variables using the Control Panel in Windows. You must restart the computer for the settings to take effect.

SERVERNODE Environment Variable

The SERVERNODE environment variable specifies the node where the NR-server resides. SERVERNODE affects all applications using CAICCI registered with the NR-server.

You usually set the SERVERNODE environment variable during installation.

RMTHOSTS Environment Variable

The RMTHOSTS environment variable specifies the hosts that can be contacted only through the remote service. RMTHOSTS affects only the CAICCI remote service.

You can use the RMTHOSTS environment variable if the local host is a bridgenode and all UNIX hosts are listed.

CCIDOMAINS Environment Variable

The CCIDOMAINS environment variable links other CAICCI servers to communicate inquiries across domains. CCIDOMAINS affects the CAICCI NR-server.

This variable can help reduce the exposure of one CAICCI server. You can break up the CAICCI domain into smaller domains and use the CCIDOMAINS environment variable to link these domains.

CA_CCITRACE Environment Variable

The CA_CCITRACE environment variable enables CAICCI tracing. CA_CCITRACE affects all applications using CAICCI services.

CA_PROTEPINDX Environment Variable

The CA_PROTEPINDX environment variable specifies the protocol where a Remote Procedure Call (RPC) runs. You can set this value to *one* of the following:

- 0 for NetBEUI
- 1 for Transmission Control Protocol (TCP). This is the default.
- 2 for User Datagram Protocol (UDP)

CA_PROTEPINDX affects the communication service. All hosts must use the same protocol.

QUENTB_PORT Environment Variable

The QUENTB_PORT environment variable specifies the listening port for RPC over NetBEUI. The default value is 202.

QUENTB_PORT affects the communication service. You can use the QUENTB_PORT environment variable to avoid opening published ports or when testing.

QUETCP_PORT Environment Variable

The QUETCP_PORT environment variable specifies the listening port for RPC over TCP. The default value is 7003.

QUETCP_PORT affects the communication service. You can use the QUETCP_PORT environment variable to avoid opening published ports or when testing.

QUEUDP_PORT Environment Variable

The QUEUDP_PORT environment variable specifies the listening port for RPC over UDP. The default value is 7001.

QUEUDP_PORT affects the communication service. You can use the QUEUDP_PORT environment variable to avoid opening published ports or when testing.

CCI_BRIDGENODE Environment Variable

The CCI_BRIDGENODE environment variable specifies the Windows node through which you can reach the UNIX hosts. CCI_BRIDGENODE affects the remote service.

You can use the CCI_BRIDGENODE environment variable if a host other than the CAICCI server is a bridgenode.

CA_QUE_RETRIES Environment Variable

The CA_QUE_RETRIES environment variable controls how long a sender waits for a target to pick up a message. This value is set in 30-second increments. The default value is 3.

CA_QUE_RETRIES affects all applications using CAICCI. You can use the CA_QUE_RETRIES environment variable if an application is busy for long periods of time (for example, when database access takes a long time to handle CAICCI messages).

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 Scheduling 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 207).

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 203).

   b. Define the local r11.3 instance on the external r11 or r11.3 instance (see page 204).

   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 87) 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
     ```

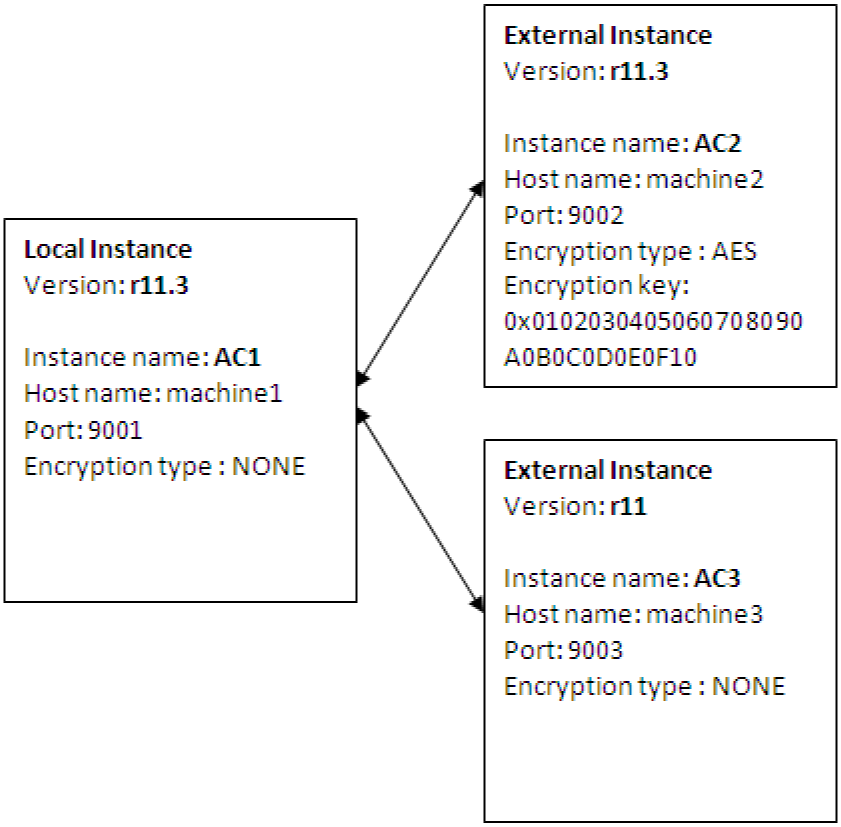
   Note: External r11 instances do not support AES encryption. To support external instance job dependencies with r11, AES encryption must be disabled on the local r11.3 instance.
3. Do *one* of the following:
   - Enter **exit** if you are using interactive mode.
   - Redirect the script to the jil command 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:



Local Instance
Version: **r11.3**

Instance name: **AC1**
Host name: machine1
Port: 9001
Encryption type : NONE

External Instance
Version: **r11.3**

Instance name: **AC2**
Host name: machine2
Port: 9002
Encryption type : AES
Encryption key:
0x0102030405060708090
A0B0C0D0E0F10

External Instance
Version: **r11**

Instance name: **AC3**
Host name: machine3
Port: 9003
Encryption type : NONE

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 Scheduling 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 209).

   b. Run the required SQL statements on the database the external r4.5 instance uses (see page 210).

   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 211).

   b. Define the external r4.5 instance on the local r11.3 instance (see page 212).

   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 87) 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 and submitting cross-instance jobs, 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 70).

   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 212).

   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)
```

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
```

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 219).
2. Set encryption for z/OS communication (see page 170).
3. (AES 128-bit encryption only) Generate an instance-wide communication alias encryption file (see page 171).
4. Define CA Workload Automation EE as an external instance (see page 224).
5. Configure the AGENTDEF data set on CA Workload Automation EE (see page 226).
6. Verify the setup (see page 228).

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. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Click the Scheduler icon on the toolbar.

   The Scheduler - CA Workload Automation AE Administrator window appears.

3. Enter the port number in the Auxiliary Listening Port field in the Communication Ports pane, and click Apply.

   The scheduler auxiliary listening port is defined. The scheduler uses this port to communicate with CA Workload Automation EE and the agent on z/OS. This port is used for all non-SSA communication.

4. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

5. Change to the %CSAM_SOCKADAPTER%\bin folder, and enter the following command:

   ```
   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 Auxiliary Listening Port field on the Scheduler - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.

   Port multiplexing and SSL encryption are disabled for the specified scheduler auxiliary listening port.

6. Do the following:

   a. Click Start, Programs, CA, Workload Automation AE, Administrator.

      The Instance - CA Workload Automation AE Administrator window opens.

   b. Select an instance from the Instance drop-down list.

   c. Click the Services icon on the toolbar.

      The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

   d. Right-click the scheduler service, and click Stop.

      The scheduler stops.

   e. Right-click the scheduler service, and click Start.

      The scheduler starts.

   The scheduler auxiliary listening port is configured.

Note: For more information about the CA Workload Automation AE Administrator, see the *Online Help*.

Set Encryption for z/OS Communication

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 clear the Use AES 128-bit encryption when communicating with zOS managers check box.
- 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

1. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select the instance you want to set encryption for from the Instance drop-down list.
3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the scheduler and application server services, and click Stop.

   The scheduler and application server stop.

5. Click the Instance icon on the toolbar.

   The Instance - CA Workload Automation AE Administrator window appears.

6. Click the zOS Encryption tab, and select the Use AES 128-bit encryption when communicating with zOS managers check box.

   The Hexadecimal Key and Verify Hexadecimal Key fields are enabled.

   Note: If you clear the Use AES 128-bit encryption when communicating with zOS managers check box, CA Workload Automation AE uses no encryption for z/OS communication.

7. Enter the encryption key, confirm the encryption key in the Verify Hexadecimal Key field, and click Apply.

   Note: The encryption key must be a hexadecimal string of 32 characters.

   The zOS Encryption Status field displays the current encryption set for the instance.

8. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

9. Right-click the scheduler and application server services, and click Start.

   The scheduler and application server start. The encryption for z/OS communication is set.

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter the following command:

   ```
   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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter **jil** at the instance command prompt.

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

3. 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.

4. 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

5. Enter **exit**.

   The data is loaded into the database. 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 216)

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
PORT(*sch_aux_port*)	Specifies the port number that the CA Workload Automation AE scheduler uses for all non-SSA communication.	Auxiliary Listening Port field on the Scheduler - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator.
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
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*.

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 a CA Workload Automation AE instance command 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 230).
2. Enable bi-directional scheduling on CA Workload Automation AE (see page 235).
3. Configure and start CAICCI (see page 236).
4. (High availability environments only) Configure failover support for cross-instance scheduling (see page 237).
5. Define the machine as an external instance on CA Workload Automation AE (see page 238).

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 local r11.3 instance, log on as the EXEC superuser and enter the following command at the instance command prompt:

   ```
   sendevent -E STOP_DEMON
   ```

   The scheduler completes any processing it is currently performing and stops.

2. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

3. Select an instance from the Instance drop-down list.

4. Click the Scheduler icon on the toolbar.

   The Scheduler - CA Workload Automation AE Administrator window appears.

5. Select Manager & Agent in the Cross Platform Scheduling pane, and click Apply.

6. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears.

7. Right-click the scheduler service, and click Start.

   The scheduler starts.

8. 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 Cross Platform Scheduling pane on the Scheduler - CA Workload Automation AE Administrator window, see the *Online Help*. For more information about the scheduler log file, 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 use cross-platform scheduling.

Note: You do not need to configure the ccirmtd file on a Windows to Windows platform environment. However, you must configure the ccirmtd file on any cross-platform environment (for example, Windows to UNIX, UNIX to mainframe, and mainframe to Windows).

To configure and start CAICCI

1. On the CA Workload Automation AE instance, log in with an account that has administrative privileges.
2. Locate and open the ccirmtd.rc 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:

   ```
   ccicntrl start
   ```

   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 agent computers (mainframe or UJMA) are sent to the secondary scheduler computer for processing.

To configure failover support for cross-instance scheduling

1. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select your instance from the Instance drop-down list.
3. Click the System icon on the toolbar.

   The System - CA Workload Automation AE Administrator window appears.

4. Double-click the PRIMARYCCISYSID variable in the Environment Variables pane.

   The window refreshes to display PRIMARYCCISYSID variable in the Variable field and its value in the Value field.

5. Enter the aliased CAICCI system ID in the Value field, and click Set.

   Note: You can find the aliased CAICCI system ID in the ccirmtd configuration file. The PRIMARYCCISYSID variable is initially configured during scheduler installation.

   The PRIMARYCCISYSID variable is modified and displayed in the Environment Variables pane.

Note: For more information about the Environment Variables pane on the System - CA Workload Automation AE Administrator window, see the *Online Help*.

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter **jil** at the instance command prompt.

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

3. 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.

4. If xcrypt_type is set to AES, specify the following additional attribute:

   ```
   xkey_to_manager: key
   ```

5. Repeat Steps 2 and 3 for each external instance that you want to communicate with.

6. Enter **exit**.

   The data is loaded into the database. 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:

Cross-Platform Scheduling Requirements (see page 230)
CA UJMA (see page 231)
CA AutoSys WA Connect Option (see page 231)
CA UJMA and CA AutoSys WA Connect Option Considerations (see page 232)
CA UJMA and CA AutoSys WA Connect Option External Instance Types (see page 233)

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 230).
2. Enable bi-directional scheduling on CA Workload Automation AE (see page 235).
3. Configure and start CAICCI (see page 236).
4. (High availability environments only) Configure failover support for cross-platform scheduling (see page 237).
5. Define the external machine on CA Workload Automation AE (see page 249).
6. (CA UJMA only) Define CA UJMA user IDs and passwords on CA Workload Automation AE (see page 250).
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 local r11.3 instance, log on as the EXEC superuser and enter the following command at the instance command prompt:

   ```
   sendevent -E STOP_DEMON
   ```

   The scheduler completes any processing it is currently performing and stops.

2. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

3. Select an instance from the Instance drop-down list.

4. Click the Scheduler icon on the toolbar.

   The Scheduler - CA Workload Automation AE Administrator window appears.

5. Select Manager & Agent in the Cross Platform Scheduling pane, and click Apply.

6. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears.

7. Right-click the scheduler service, and click Start.

   The scheduler starts.

8. 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 Cross Platform Scheduling pane on the Scheduler - CA Workload Automation AE Administrator window, see the *Online Help*. For more information about the scheduler log file, 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 use cross-platform scheduling.

Note: You do not need to configure the ccirmtd file on a Windows to Windows platform environment. However, you must configure the ccirmtd file on any cross-platform environment (for example, Windows to UNIX, UNIX to mainframe, and mainframe to Windows).

To configure and start CAICCI

1. On the CA Workload Automation AE instance, log in with an account that has administrative privileges.
2. Locate and open the ccirmtd.rc 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:

   ```
   ccicntrl start
   ```

   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 agent computers (mainframe or UJMA) are sent to the secondary scheduler computer for processing.

To configure failover support for cross-instance scheduling

1. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select your instance from the Instance drop-down list.

3. Click the System icon on the toolbar.

   The System - CA Workload Automation AE Administrator window appears.

4. Double-click the PRIMARYCCISYSID variable in the Environment Variables pane.

   The window refreshes to display PRIMARYCCISYSID variable in the Variable field and its value in the Value field.

5. Enter the aliased CAICCI system ID in the Value field, and click Set.

   Note: You can find the aliased CAICCI system ID in the ccirmtd configuration file. The PRIMARYCCISYSID variable is initially configured during scheduler installation.

   The PRIMARYCCISYSID variable is modified and displayed in the Environment Variables pane.

Note: For more information about the Environment Variables pane on the System - CA Workload Automation AE Administrator window, see the *Online Help*.

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. Click Start, Programs, CA, Workload Automation AE, Command Prompt (*instance_name*).

   The CA Workload Automation AE instance command prompt opens.

2. Enter **jil** at the instance command prompt.

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

3. 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.

4. Enter **exit**.

   The data is loaded into the database. 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*.

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.
- The scheduler and application server installations for an instance must have the same event server settings in the CA Workload Automation AE Administrator.

How to Install Dual Event Servers

The following steps ensure a successful installation of the dual event servers:

1. Identify two computers on which to install the event servers (databases) (see page 254).
2. Stop the scheduler (see page 255).
3. Stop the application server (see page 255).
4. Install and configure the event servers on each computer. (see page 256)
5. Use the CA Workload Automation AE Administrator to associate the two event servers (see page 256).
6. Synchronize the databases (see page 257).
7. Start the scheduler (see page 262).
8. Start the application server (see page 263).

More information:

autobcpDB Script—Synchronize Databases (see page 258)

Identify Two Computers

If you are already running CA Workload Automation AE with a single event server, select an additional event server computer on which to install the second event server. Otherwise, identify two computers and install an event server on each computer.

Stop the Scheduler

You must stop the scheduler before you set up dual event server mode.

To stop the scheduler

1. Log on to the scheduler computer as the EXEC superuser.
2. Enter the following command:

   ```
   sendevent -E STOP_DEMON
   ```

   The scheduler stops.

Note: When you stop the scheduler, any jobs that are running run to completion. You can continue with the remaining steps while the jobs are completing.

Stop the Application Server

You must stop the application server before you set up dual event server mode.

To stop the application server

1. Open the CA Workload Automation AE Administrator from your CA Workload Automation AE program group.

   The Instance - CA Workload Automation AE Administrator window appears.
2. Select an instance from the Instance drop-down list.
3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.
4. Right-click the application server, and click Stop.

   The application server stops.

To verify that the application server has stopped, check the Status column on the Services - CA Workload Automation AE Administrator window. The Status column should read Stopped.

Note: If you have more than one application server configured for your enterprise, you must follow these steps for all computers running as application servers before proceeding with configuring dual event servers.

Install and Configure the Event Servers

You can install and configure your own database for your event servers.

Note: You must select the Standalone option on the Installation Function page if you want to create the second event server to run CA Workload Automation AE in dual event server mode. Make sure that your event servers are of the same type and your databases are configured for CA Workload Automation AE.

Start Event Servers

After you install and configure the event servers, make sure that both the event servers are started.

Associate the Two Event Servers

For the scheduler and application server installations, you must set the event server settings so that these components can communicate with both the databases. During installation, the setup wizard lets you set up the dual event servers. Use the GUI to view and modify these settings after installation.

If you did not use the setup wizard, you must configure your event servers and create a dual event server mode relationship between the individual databases you installed.

To set up a dual event server mode, if you have already installed CA Workload Automation AE and are adding a second database, use the following steps for each computer on which the instance is installed (you must have Windows Administrators group privileges).

To set up a dual event server mode

1. Ensure that the scheduler and the application server are not running.
2. Open the CA Workload Automation AE Administrator from your CA Workload Automation AE program group.

   The Instance - CA Workload Automation AE Administrator window appears.
3. Select an instance from the Instance drop-down list.

   Note: If you have Windows Administrators group privileges, you can use the Instance - CA Workload Automation AE Administrator window to connect to other computers on which the instance is installed. You must perform the following steps for each instance installed.
4. Click the Event Server icon on the toolbar.

   The Event Server - CA Workload Automation AE Administrator window appears.

5. Enter the server information for the new second database in the Event Server B area, and click Enable.

   The database mode changes from single event server to dual event server mode.

6. Click Apply.

   Your changes are saved.

More information:

Synchronize the Databases (see page 257)

Synchronize the Databases

Before you start the scheduler, you must synchronize the event server databases. CA Workload Automation AE provides an autobcp*DB* script to synchronize both of the event server databases. This script identifies one database as the source and the other database as the target for the synchronization process.

Before you synchronize the event servers, check the following:

- Ensure that both the event servers are running.
- Ensure that no CA Workload Automation AE schedulers, application server or GUI applications are running.
- Ensure that your event servers have unique names (for example, eventserver1::AEDB and eventserver2::AEDB).
- For Microsoft SQL Servers, ensure that both the databases are defined correctly. Use the Microsoft SQL Enterprise Manager to view the information.
- For Oracle, ensure that the TNSNAMES.ORA file contains valid entries for both the event servers.
- For Sybase, ensure that the SQL.INI file contains entries for both the event servers.
- Know the path to the database software, so you can supply it when you run the autobcp*DB* script.
- Ensure that you have at least as much free disk space as the size of your database for the temporary file that autobcp*DB* script creates. The script deletes this temporary file after the synchronization process is complete.

Note: 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 the 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 the event servers.

You can also use this procedure to return to a dual event server mode if CA Workload Automation AE went into a single event server mode due to a database rollover.

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:

  ```
  C:\PROGRA~1\CA\UNICEN~1> set 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.

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.

Depending on your database, run the following script:

- autobcpMSQ.pl (for Microsoft SQL Server)
- autobcpORA.pl (for Oracle)
- autobcpSYB.pl (for Sybase)

The autobcp*DB* script is located at C:\Program Files\CA\WorkloadAutomationAE\autosys\dbobj\dbtype.

dbtype

Specifies the type of database in use: MSQ (Microsoft SQL Server), ORA (Oracle), or SYB (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 Microsoft SQL Server

```
perl autobcpMSQ.pl source_server source_db target_server target_db source_userid
source_password target_userid target_password dump_file
```

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 Microsoft SQL Server, 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. For Microsoft SQL Server, you must use the Client Network Utility to define the source server.

source_db

Defines the source Microsoft SQL Server or Sybase database (for example, AEDB).

source_userid

Defines the user ID that is used to connect to the source Microsoft SQL Server, Oracle System ID, or Sybase server.

Note: For Oracle, you must use aedbadmin as the source user ID.

source_password

Defines the password that corresponds to the user ID that is used to connect to the source Microsoft SQL Server, Oracle System ID, or Sybase server.

target_server

Defines the target Microsoft SQL Server, 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. For Microsoft SQL Server, you must use the Client Network Utility to define the target server.

target_db

Defines the target Microsoft SQL Server or Sybase database (for example, AEDB2).

target_userid

Defines the user ID that is used to connect to the target Microsoft SQL Server, Oracle System ID, or Sybase server.

Note: For Oracle, you must use aedbadmin as the target user ID.

target_password

Defines the password that corresponds to the user ID that is used to connect to the target Microsoft SQL Server, 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 (MyComputer) and the target server (MyComputer).

Note: If you use the target user ID with the truncate command, the data is copied faster and reduces the database log requirements.

```
>perl autobcpMSQ.pl MyComputer AEDB MyComputer AEDB2 autosys autosys sa autosys
dump.txt
```

Handle Errors

If the autobcp*DB* script detects an error, it exits and displays the following message:

```
The AutoSys data server is not accessible.
Please check the data server and rerun this script.
```

If this happens, check the following, and rerun the autobcp*DB* script:

- Are both event servers started?

  To verify this, look at the Windows Control Panel Services dialog, and verify that the status of the database service is Started.

  - For a Microsoft SQL Server, the service name is MSSQLServer (you can also check this service using the Microsoft SQL Service Manager).
  - For Oracle databases, look for the following three services (substitute the Oracle SID for the asterisk): OracleService*, OracleStart*, and OracleTNSListener.
  - For Sybase, the service name is user-configurable. You must connect to the Sybase server using the isql utility.
- Did you specify the source and the target databases correctly in the autobcp*DB* script?
- Did you enter the passwords correctly in the autobcp*DB* script?
- Did you set the Oracle or Sybase environment variables correctly?
  - The Oracle environment variable, ORACLE_HOME, defines the path to the top-level Oracle directory.
  - The Sybase environment variables are DSQUERY and SYBASE. The DSQUERY variable defines the name of the Sybase event server. The SYBASE variable defines the complete path to the Sybase software directory.
- Did you specify the event server names and ports correctly?
  - For Microsoft SQL Server, you specify this information during installation while using the SQL Setup program. Use the Microsoft SQL Enterprise Manager to view this information.
  - For Oracle, this information is located in the TNSNAMES.ORA file.
  - For Sybase, this information is located in the SQL.INI file.

Note: The scheduler marks both the event servers as being in dual event server mode. CA Workload Automation AE client processes and commands check the flags in both the event servers for consistency; therefore, you must start the scheduler before running any other commands.

More information:

Start the Scheduler (see page 262)

Start the Scheduler

To start the scheduler, you must have Windows Administrators group privileges.

To start the scheduler

1. Open the CA Workload Automation AE Administrator from your CA Workload Automation AE program group.

   The Instance - CA Workload Automation AE Administrator window appears.

2. Select an instance from the Instance drop-down list.
3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the scheduler, and click Start.

   The scheduler starts.

To verify that the scheduler has started, check the Status column on the Services - CA Workload Automation AE Administrator window. The Status column should read Running.

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

In addition, you can monitor the scheduler output by entering the autosyslog -e command at a CA Workload Automation AE instance command prompt. To stop the autosyslog command, press Ctrl+C.

Note that when changing the dual event server configuration, the scheduler must be started before any other application as it updates the database as to the dual event server status of the enterprise. This includes the application server. Without the application server, it is impossible to run any client processes. If you choose to run autoping or chk_auto_up command before starting your scheduler, you must set the AS_TXLOCAL=1 environment variable to let the client application bypass the application server. This must be done in a specific command prompt to avoid applying it to all client applications. Unset the AS_TXLOCAL environment variable or close the command prompt in which it is set to avoid inadvertently bypassing the application server.

Start the Application Server

To start the application server, you must have Windows Administrators group privileges.

To start the application server

1. Open the CA Workload Automation AE Administrator from your CA Workload Automation AE program group.

   The Instance - CA Workload Automation AE Administrator window appears.

2. Select an instance from the Instance drop-down list.
3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the application server, and click Start.

   The application server starts.

To verify that the application server has started, check the Status column on the Services - CA Workload Automation AE Administrator window. The Status column should read Running. You must do this on each computer that is running an application server.

Note: When changing dual event server status, the application server fails to start if the scheduler has not already been started.

Shadow and Tie-Breaker Schedulers

CA Workload Automation AE provides high availability through a shadow scheduler or by using the dual event servers. 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 or Tie-Breaker 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. If you run CA Workload Automation AE with a shadow scheduler and dual event servers, a tie-breaker scheduler is required.

To install a shadow scheduler or a tie-breaker scheduler

1. Install a scheduler, application server, and an agent (the application server and agent are installed automatically with a scheduler) on the computers where the shadow scheduler or 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 administrator settings on the primary, shadow, and tie-breaker computers to specify the type of scheduler the computer will be. To do this, follow these steps:

   a. Open the CA Workload Automation AE Administrator from your CA Workload Automation AE program group.

      The Instance - CA Workload Automation AE Administrator window appears.

   b. Select an instance from the Instance drop-down list.

   c. Click the Scheduler icon on the toolbar.

      The Scheduler - CA Workload Automation AE Administrator window appears.

   d. Select the scheduler role in the Scheduler Role pane, and click Apply

      The selected scheduler role is applied to the computer.

3. Use the Services - CA Workload Automation AE Administrator window to start the scheduler service for the primary, shadow, and tie-breaker computers.

4. Enter autosyslog -e command at a CA Workload Automation AE instance command 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. Open the CA Workload Automation AE Administrator from your CA Workload Automation AE program group.

   The Instance - CA Workload Automation AE Administrator window appears.

2. Select an instance from the Instance drop-down list.

3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the scheduler service, and click Stop.

   The scheduler stops.

5. Right-click the scheduler service, and click Start.

   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.

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 CA Workload Automation AE Administrator, you must set the following fields when configuring CA Workload Automation AE in high availability mode:

Scheduler Role

Specifies whether the scheduler is a primary, shadow, or tie-breaker scheduler.

HA Poll Interval

Checks if any schedulers have gone down in the seconds specified.

Application Server Host

Tells the agents to return events to the correct application server. This value is used when a rollover occurs from primary to shadow scheduler.

Note: This applies to legacy agents only.

Event Server

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, application server, and agent on computer1.
2. Stop the scheduler, application server, and agent on computer2.
3. Set the following fields in the CA Workload Automation AE Administrator on computer1:
    a. Scheduler Role to Primary
    b. HA Poll Interval to 5
    c. Application Server Host to computer1, computer2
    d. Event server A to AEDB
4. Ensure database connectivity exists on computer 2 to event server A, which resides on computer1.

5. Set the following fields in the CA Workload Automation AE Administrator on computer2:

   a. Scheduler Role to Shadow

   b. HA Poll Interval to 5

   c. Application Server Host to computer1, computer2

   d. Event server A to computer1::AEDB

6. Start the agent, scheduler, and application server on computer1.

7. Start the agent, scheduler, and application server on computer2.

8. Run autosyslog –e command on computer1. The following output is displayed:

   ```
   -
   [08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in single server
   mode.  Event server A:  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.
   -
   ```

9. Run autosyslog –e command on computer2. The following output is displayed:

   ```
   -
   [08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in single server
   mode.  Event server A:  computer1::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: The environment is now in high availability mode. If you make changes to the configuration, you must stop the schedulers and application servers.

10. Stop the scheduler and the application server using the Services - CA Workload Automation AE Administrator window on computer2.

11. Run 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.
    -
    ```

    The shadow scheduler performs a normal shutdown and the primary scheduler acknowledges this. The shadow scheduler can be started again and CA Workload Automation AE resumes in high availability mode.

More information:

Start the Scheduler (see page 262)
Start the Application Server (see page 263)
Stop the Scheduler (see page 255)
Stop the Application Server (see page 255)

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 CA Workload Automation AE Administrator, you must set the following fields when configuring CA Workload Automation AE in high availability mode with dual event servers:

Scheduler Role

Specifies whether the scheduler is a primary, shadow, or tie-breaker scheduler.

HA Poll Interval

Checks if any schedulers have gone down in the seconds specified.

Application Server Host

Tells the agents to return events to the correct application server. This value is used when a rollover occurs from primary to shadow scheduler.

Note: This applies to legacy agents only.

Event Server

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, which may or may not be configured:

1. Stop the scheduler, application server, and agent on computer1.
2. Stop the scheduler, application server, and agent on computer2.
3. Stop the scheduler, application server, and agent on computer3.
4. Ensure database connectivity exists on computer 1 to event server B, which resides on computer2.
5. Set the following fields in the CA Workload Automation AE Administrator on computer1:
    a. Scheduler Role to Primary
    b. HA Poll Interval to 5
    c. Event Reconnect to 50,5
    d. Application Server Host to computer1, computer2, computer3 (if applicable)
    e. Event server A to AEDB
    f. Event server B to computer2::AEDB

6. Ensure database connectivity exists on computer2 to event server A, which resides on computer1.
7. Set the following fields in the CA Workload Automation AE Administrator on computer2:
    a. Scheduler Role to Shadow
    b. HA Poll Interval to 5
    c. Event Reconnect to 50,5
    d. Application Server Host to computer2, computer1, computer3 (if applicable)
    e. Event server A to computer1::AEDB
    f. Event server B to AEDB
8. Ensure database connectivity exists on computer3 to event server A, which resides on computer1 and to event server B, which resides on computer2.
9. Set the following fields in the CA Workload Automation AE Administrator on computer3:
    a. Scheduler Role to Tie-breaker
    b. HA Poll Interval to 5
    c. Event Reconnect to 50,5
    d. Application Server Host to computer3 (if applicable), computer1, computer2
    e. Event server A to computer1::AEDB
    f. Event server B to computer2::AEDB
10. Start the agent, scheduler, and application server on computer1.
11. Start the agent, scheduler, and application server on computer2.
12. Start the agent, scheduler, and application server on computer3.

13. Run autosyslog –e command on computer1. The following output is displayed:

    ```
    -
    [08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in dual server
    mode.  Event server A:  AEDB.  Event server B:  computer2::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.
    -
    ```

14. Run autosyslog –e command on computer2. The following output is displayed:

    ```
    -
    [08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in dual server
    mode.  Event server A:  computer1::AEDB.  Event server B:  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.
    -
    ```

15. Run autosyslog –e command on computer3. The following output is displayed:

    ```
    -
    [08/08/2005 10:46:01]      CAUAJM_I_10654 System is running in dual server
    mode.  Event server A:  computer1::AEDB.  Event server B:  computer2::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: The environment is now in high availability mode with dual event servers employed. If you make changes to the configuration, you must stop the schedulers and application servers.

16. Stop the scheduler and the application server using the Services - CA Workload Automation AE Administrator window on computer2.

17. Run 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.
    -
    ```

    The shadow scheduler performs a normal shutdown and the primary scheduler acknowledges this. The shadow scheduler can be started again and CA Workload Automation AE resumes in high availability mode. The same is true when a tie-breaker scheduler performs a normal shutdown; the primary scheduler acknowledges this. The tie-breaker scheduler can be started again and CA Workload Automation AE resumes in high availability mode.

Set Up CA Workload Automation AE in a High-Availability Cluster Environment

CA Workload Automation AE can be installed in a Microsoft Cluster Server Environment to form a highly-available CA Workload Automation AE scheduler and application server. The CA Workload Automation AE highly-available configuration promotes minimal down time and uses resources optimally to make sure that your enterprise is continuously monitored and managed.

A highly-available CA Workload Automation AE scheduler and application server require a highly-available database. You must set up a highly-available database before proceeding with the CA Workload Automation AE installation on a cluster node. The procedures for preparing a highly-available database vary depending on the database used.

Note: For information about the databases, refer to the documentation for those databases.

When setting up CA Workload Automation AE to be highly-available, keep the following in mind:

- CA Workload Automation AE agent service is not to be defined as a cluster service. The agent service gets installed on each of the private disks, independent of the cluster system.
- CA Workload Automation AE application server and scheduler always run in *active/passive* mode and are defined as a cluster service. 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.
- The %AUTOSYS% and %AUTOUSER% directories are installed on the non-shared disk. After installation, you can optionally change the %AUTOUSER% directory to point to a shared disk, if you want to access the log files from any cluster.

Note: For more information about configuring and managing a Microsoft Cluster Server, see the Microsoft Cluster Server documentation.

To set up CA Workload Automation AE to be highly-available

1. Install cluster software on each computer in the cluster.
2. Use the following steps for each database vendor:

   Microsoft SQL Database

   > Select one instance of a Microsoft SQL Server cluster resource group to use for CA Workload Automation AE. The highly-available service uses the related network name and IP address as set up from the Microsoft SQL Server installation.
   >
   > **Note:** In the following steps, "CA Workload Automation AE resource group" refers to the Microsoft SQL Server cluster resource group you are using for CA Workload Automation AE.

   Oracle Database

   > Select one instance of an Oracle cluster resource group to use for CA Workload Automation AE. The highly-available service uses the related network name and IP address as set up from the Oracle installation.
   >
   > **Note:** In the following steps, "CA Workload Automation AE resource group" refers to the Oracle resource group you are using for CA Workload Automation AE.

   Sybase Database

   > Select one instance of a Sybase cluster resource group to use for CA Workload Automation AE. The highly-available service uses the related network name and IP address as set up from the Sybase installation.
   >
   > **Note:** In the following steps, "CA Workload Automation AE resource group" refers to the Sybase cluster resource group you are using for CA Workload Automation AE.

3. On the first node in the cluster, install CA Workload Automation AE and all of the components you want to use.

   The highly-available service is installed automatically as part of CA common components or on a clustered computer where cluster software is present. For example, on Windows, the highly-available service is installed on a computer where Microsoft Cluster Server is running. The highly-available service detects that the computer is in a cluster and a dialog box appears that lists all of the resource groups in the cluster.

   Important! To make sure that the highly-available service works across the nodes of your cluster, you must run the highly-available service under a cluster domain account on Windows.

4. Select the CA Workload Automation AE resource group.

   Depending on the components you installed, the following CA Workload Automation AE resources are added to the resource group:

   - CA Workload Automation AE Application Server
   - CA Workload Automation AE Scheduler

   Because all of the CA Workload Automation AE resources belong to one resource group, all of them fail over at the same time.

   Note: The CA Workload Automation AE resources are managed by the Cluster Administrator. During the installation, the option to autostart these services is disabled.

5. After the installation completes on the first node, perform the following tasks:

   a. Verify that the CA Workload Automation AE resources (CA CA Workload Automation AE Application Server and CA CA Workload Automation AE Scheduler) are offline.

   b. Move the CA Workload Automation AE resource group over to a subsequent node in the cluster that does not yet have CA Workload Automation AE installed on it.

6. Ensure that the cluster resources (virtual IP, virtual network name, and shared disk) are still online.

7. On all subsequent nodes in the cluster, install CA Workload Automation AE and the same components you installed on the first node.

   The highly-available service is installed automatically.

8. After the installation completes on each subsequent node, perform the following tasks:

    a. Verify that the CA Workload Automation AE resources are offline.

    b. Move the CA Workload Automation AE resource group over to a subsequent node in the cluster that does not yet have CA Workload Automation AE installed on it. The resource group must be present on the node before you can install CA Workload Automation AE.

    Note: If this is the last node in the cluster, you need not move the resource group.

9. After CA Workload Automation AE is installed on all nodes in the cluster, bring the CA Workload Automation AE resources online.

    CA Workload Automation AE is now running in a highly-available mode.

Note: If you install CA common components on a standalone computer and then add the computer to a cluster, the highly-available service or daemon does not start automatically. You must manually start the highly-available service or daemon or restart the computer.

Chapter 20: Configuring CA Workload Automation AE to Work with Other CA Products

This section contains the following topics:

Notification Services Integration

You can integrate CA Workload Automation AE with the Notification Services component of CA NSM to send wired and wireless messages, using protocols and devices, to operators or administrators who resolve problems or attend to emergencies.

Note: The Notification Services component of CA NSM is different from Wireless Messaging, which is available in Event Management. Wireless Messaging lets you send emails and pages.

The following protocols are available:

Email - SMTP, POP3

Simple Mail Transfer Protocol (SMTP) is used to send one-way and two-way email messages to various devices, including cellular telephones. Post Office Protocol version 3 (POP3) is used to receive emails from a mail server.

Wireless - WCTP

Wireless Communications Transfer Protocol (WCTP) uses XML over Hypertext Transport Protocol (HTTP) to send and receive messages and binary data between wire-line systems and one-way or two-way wireless devices.

Page - SNPP

Simple Network Paging Protocol (SNPP) is based on TCP/IP and offers one-way and two-way paging.

Page - TAP

Telocator Alphanumeric Protocol (TAP) is used to send pages by modem and is the oldest one-way paging protocol.

Short Message - SMS

Short Message Service (SMS) is used to send one-way text messages to cellular telephones using HTTP.

Instant Message - Sametime

IBM Lotus Instant Messaging and Web Conferencing (Sametime Instant Messaging - SIM) is used on Windows to send one-way and two-way instant messages.

Voice - TAPI

Telephony Application Programming Interface (TAPI) is used on Windows to send one-way voice messages that are synthesized from text using the Microsoft Speech Application Programming Interface (SAPI) text-to-speech (TTS) engine. The default speech is set in the Windows Control Panel. The messages travel by telephone line to a human recipient using a TAPI-compliant telephony device.

Script

Third-party or customer programs or scripts can be used to send one-way messages. Scripts and command definitions are stored in the UNSConnections.ini file in the install_path/config directory.

How Notification Services Works

The Notification Services component of CA NSM uses the following process to track all notifications that you send. This is important for two-way notifications that must be matched with responses.

1. You use one of the following features to create a notification message:
   - User interface
   - Command line or script
   - Event Console (by right-clicking a message)
   - Event Management NOTIFY action
   - Alert Management escalation
   - Application using the Notification Services Client SDK
2. Based on the recipient, provider, or protocol information in the request, the Notification Services daemon (unotifyd) selects a protocol-specific driver to send the notification.

   Note: The daemon runs as a service on Windows and as a background process on UNIX.
3. The daemon assigns a tracking ID, which it returns to the command or program that sent the notification.

   Note: If the daemon stops and restarts, it also restarts the outstanding notifications stored on disk.
4. The daemon periodically checks for a response from the service provider, if one was requested.
5. The daemon stores information about the notification on disk, and updates that information throughout the life cycle of the notification. This is named *checkpointing*. Updates occur for the following events:
   - The request is created.
   - The service provider received the notification.
   - The provider delivered the notification.
   - The recipient read the notification.
   - The recipient sent a reply.

How to Integrate CA Workload Automation AE with Notification Services Component of CA NSM

This topic provides an overview of the steps that you must perform to integrate CA Workload Automation AE with the Notification Services component of CA NSM.

Important! Do not install Notification Services from the Unicenter NSM r11 media. This configuration is not supported because the Unicenter NSM r11 media also installs a previous version of SSA. CA Workload Automation AE cannot work properly with the previous version of SSA installed.

Notes:

- CA Workload Automation AE requires Notification Services from CA NSM r11.2 or higher.
- By default, the Notification Services integration is inactive.

To integrate CA Workload Automation AE with the Notification Services component of CA NSM, follow these steps:

1. Install a Notification Agent on the CA Workload Automation AE server from the CA NSM media.

   Notes:

   - The Notification Agent installation assumes that you have a Notification Manager installed in your enterprise. If you do not have a Notification Manager installed, you can install the Notification Manager from the CA NSM media.
   - If the Notification Manager is not installed locally on the CA Workload Automation AE server, the Notification Agent requires a valid CAICCI connection to the Notification Manager.

2. Configure CA Workload Automation AE to work with the Notification Services component of CA NSM (see page 283).
3. Send notifications using CA Workload Automation AE (see page 284).

   Note: CA Workload Automation AE requires the node name of the Notification Manager to send a notification request to the Notification Services component of CA NSM.

Note: For more information about the Notification Services setup and configuration, see the CA NSM documentation.

Configure CA Workload Automation AE to Work with Notification Services Component of CA NSM

After installing and configuring the Notification Services component of CA NSM, you must configure the CA Workload Automation AE server to activate its notification interface.

The NotifyServerNode and NotifyAckTimeout parameters let you activate the Notification Services interface. When you set these notification parameters, the scheduler can send a notification to the Notification Services component of CA NSM if the job the scheduler is processing was defined with the appropriate notification attributes.

To configure CA Workload Automation AE to work with the Notification Services component of CA NSM

1. Log on to a CA Workload Automation AE computer as the EXEC Superuser and enter the following command at the instance command prompt:

   ```
   sendevent -E STOP_DEMON
   ```

   The scheduler completes any processing it is currently performing and stops.

2. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

3. Select an instance from the Instance drop-down list.
4. Click the Integration icon on the toolbar.

   The Integration - CA Workload Automation AE Administrator window appears.

5. Complete the following fields in the Notification pane, and click Apply:

   Server Node

   > Identifies the computer name of the Notification Services server.
   >
   > **Note:** On UNIX, the equivalent configuration parameter is NotifyServerNode.

   Timeout

   > Defines the time-out (in seconds) the client uses when requiring an acknowledgement from the Notification Services server.
   >
   > **Default:** 30. This default is sufficient for the server to respond to a client request.
   >
   > **Note:** On UNIX, the equivalent configuration parameter is NotifyAckTimeout.

6. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears.

7. Right-click the scheduler service, and click Start.

   The scheduler starts. CA Workload Automation AE is configured to work with the Notification Services component of CA NSM, and you can now send notification requests.

Send Notifications Using CA Workload Automation AE

The integration of the Notification Services component of CA NSM and CA Workload Automation AE lets you send wired and wireless messages based on the completion of a job. When a job is defined to send a notification, the CA Workload Automation AE scheduler sends the notification during terminal status processing. The scheduler prepares and sends the notification request. Messages are written to the scheduler log indicating whether the notification request was sent and processed successfully.

To send notifications using CA Workload Automation AE, specify the following attributes in the job definition:

- send_notification
- notification_id
- notification_msg

Note: For more information about the notification job attributes, see the *Reference Guide* and the *User Guide*.

Example: Send a Notification Request when a Job Completes

This example sends a notification request to a recipient named administrator when job notify_on_completion completes.

```
insert_job: notify_on_completion
machine: localhost
command: sleep 1
owner: user@localhost
send_notification: y
notification_id: administrator
notification_msg: “notify_on_completion has completed.”
```

Example: Send a Notification Request when a Job Fails

This example sends a notification request to a recipient named operator when job notify_on_failure fails.

```
insert_job: notify_on_failure
machine: localhost
command: false
owner: notify@localhost
send_notification: f
notification_id: operator
notification_msg: “notify_on_failure has failed.”
```

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 286).
2. Initiate a Service Desk ticket using CA Workload Automation AE (see page 288).

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. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

5. Select an instance from the Instance drop-down list.

6. Click the Integration icon on the toolbar.

   The Integration - CA Workload Automation AE Administrator window appears.

7. Complete the following fields in the Service Desk pane as appropriate, and click Apply:

   Web Service Login ID

   Defines the user name that is used to connect to the CA Service Desk web service.

   Note: On UNIX, the equivalent configuration parameter is ServiceDeskUser.

   Web Service Login Password

   Defines the password associated with the Web Service Login ID.

   Note: On UNIX, the equivalent configuration parameter is ServiceDeskUser.

   Web Service Customer

   (Optional) Defines the customer name for the web service.

   Notes:

   - The Web Service Customer field can be substituted for the Web Service Login ID and Web Service Login Password fields. That is, if you use a web service customer to access CA Service Desk, you can update the Web Service Customer field instead of the Web Service Login ID and Web Service Login Password fields.
   - On UNIX, the equivalent configuration parameter is ServiceDeskCust.

   URL Location

   Defines the address for CA Service Desk web service.

   Note: On UNIX, the equivalent configuration parameter is ServiceDeskURL.

8. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears.

9. Select the scheduler service, and click the Pause Service icon on the toolbar.

   The scheduler service pauses.

10. Click the Start/Resume Service icon on the toolbar.

    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 URL Location and Web Service Login ID and password values, 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. Click Start, Programs, CA, Workload Automation AE, Administrator.

   The Instance - CA Workload Automation AE Administrator window opens.

2. Select an instance from the Instance drop-down list.
3. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears, displaying a list of services installed on the selected instance.

4. Right-click the scheduler and application server services, and click Stop.

   The scheduler and application server stop.

5. Click the Integration icon on the toolbar.

   The Integration - CA Workload Automation AE Administrator window appears.

6. Complete the following fields in the Spectrum Automation Manager pane as appropriate, and click Apply:

   Web Service Login ID

   > Defines the user name that is used to connect to the CA Spectrum Automation Manager web service.
   >
   > **Note:** On UNIX, the equivalent configuration parameter is DCAUser.

   Web Service Login Password

   > Defines the password associated with the Web Service Login ID.
   >
   > **Limits:** Up to 32 characters
   >
   > **Note:** On UNIX, the equivalent configuration parameter is DCAUser.

URL Location

Defines the address for the CA Spectrum Automation Manager web service.

Example: https://dcamanager:443/dpm/sc

Notes:

- You can access CA Spectrum Automation Manager using https://dcahostname:8443/UI/DPMUI.html.
- On UNIX, the equivalent configuration parameter is DCAURL.

7. Add the Spectrum Automation Manager SDK library to the system PATH environment variable from My Computer, Properties, Advanced, Environment Variables.

   The PATH environment variable is modified to include the directory where the SDK libraries reside.

8. Click the Services icon on the toolbar.

   The Services - CA Workload Automation AE Administrator window appears.

9. Right-click the scheduler service, and click Start.

   The scheduler starts and writes Spectrum Automation Manager specific information to the CA Workload Automation AE database.

10. Right-click the application server service, and click Start.

    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.

Chapter 21: 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.
- 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
- During the CA Workload Automation AE upgrade, if SSA or any other application using SSA is active, the upgrade fails to change any SSA related binaries or libraries and you may have to restart your computer to complete the CA Workload Automation AE upgrade. If you must restart your computer, the installer displays the option to restart your computer during the CA Workload Automation AE upgrade.

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 Windows computer.

To upgrade Unicenter AutoSys JM on a Windows computer

1. Log in as a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.
3. Run the installation program using the following command:

   ```
   setup.exe
   ```

   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 Microsoft SQL Server as the database type, go to Specify Microsoft SQL Server Database Properties (see page 298) section to continue.
    - If you selected Oracle as the database type, go to the Specify Oracle Database Properties (see page 299) section to continue.
    - If you selected Sybase as the database type, go to the Specify Sybase Database Properties (see page 301) 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 Microsoft SQL Server Database Properties

If you selected the Microsoft SQL Server 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 Microsoft SQL Server database properties

1. Enter the Microsoft SQL Server name and the database name, select whether to create the CA Workload Automation AE database and whether to use Windows authentication, and Click Next.

   Note: If you select the Use SQL Server authentication check box, you must specify the SA user name and password.

   The Primary Event Server Properties page appears.

2. Enter the CA Workload Automation AE database user name and password, and click Next.

   One of the following occurs:

   - If you selected the Employ Dual Event Servers check box on the CA Workload Automation Database Properties page, the Secondary Event Server Properties page appears. Continue with Step 3.
   - If you did not select the Employ Dual Event Servers check box on the CA Workload Automation Database Properties page, the Scheduler Properties page appears. Continue with Step 4.

3. Enter the Microsoft SQL Server name and the database name for the second event server, select whether to create the CA Workload Automation AE database and whether to use Windows authentication, and click Next.

   Note: If you select the Use SQL Server authentication check box, you must specify the SA user name and password.

   The Scheduler Properties page appears.

4. Enter the scheduler properties as appropriate, and click Next.

   The Database Test page appears.

5. Click Start Test to verify the existence of the Microsoft SQL Server database and the validity of the connection information.

   The results of the test are displayed.

6. If the test is successful, click Next.

   The page appears.

   Note: If the test fails, click Back to correct the connection information.

7. Return to the main upgrade procedure and continue with the upgrade.

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 295)

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 295)

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: sleep 10
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 22: 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
Microsoft SQL Server 7, 2000, or 2005	Microsoft SQL Server 2005 or 2008
Oracle 8.17, 9.2, 10g, or 11g	Oracle 9.2, 10g, or 11g
Sybase 11.9.2, 11.9.3, 12.0, or 12.5	Sybase 12.5.2 or 15.0

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 310)
Download Database JAR Files (see page 313)
Determine the Native JDBC JAR Path (see page 312)

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 310).
2. Locate the TCP/IP database listener port number (see page 310).
3. Determine the native JDBC JAR path (see page 312).
4. Download the database JAR files (see page 313).
5. Invoke the migration utility (see page 313).
6. Stop the migration utility (see page 316).

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 Microsoft SQL Server

To find the TCP/IP port for Microsoft SQL Server

1. Start SQL Query Analyzer, and connect to the instance of Microsoft SQL Server.

   Note: If you have installed CA Workload Automation AE on Microsoft SQL Server 2008, you must use SQL Server Management Studio to query the database.

2. Run the following Transact-SQL statement in SQL Query Analyzer:

   ```
   Use master
   Go
   Xp_readerrorlog
   ```

   The Results pane appears.

3. Locate the following text:

   SQL server listening on *X.X.X.X*: *Y*

   X.X.X.X

   Indicates the IP address of the instance of Microsoft SQL Server.

   Y

   Indicates the TCP/IP port where Microsoft SQL Server is listening.

   Note: The default port number is 1433.

Example: Microsoft SQL Server TCP/IP port

Suppose the text reads 10.150.158.246: 1433. This means that

10.150.158.246

indicates the IP address of the Microsoft SQL Server, and

1433

indicates the TCP/IP port where the instance of Microsoft SQL Server is listening.

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 Microsoft SQL Server, Oracle, and Sybase database types. The following tables list native JDBC JAR files and their example sample paths:

SQL Server: Microsoft SQL Server 2005 JDBC Drivers

JDBC JAR	Example Path
qljdbc.jar	C:\Program Files\MSSQL 2005 JDBC\MicrosoftSQLServer2005JDBCDrivers\sqljdbc_1.0\enu\sqljdbc.jar

Oracle: Oracle Database 10g JDBC Drivers

JDBC JAR	Example Path
classes12.jar	C:\oracle\product\10.1.0\Db_1\jdbc\lib\classes12.jar

Sybase: Sybase jConnect for JDBC Version 6.0

JDBC JAR	Example Path
jconn3.jar	C:\sybaseASE15.0\jConnect-6_0\classes\jconn3.jar

Note: The migration utility needs access to these JAR files so it can 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 the CA Workload Automation AE instance command prompt.
2. Stop the scheduler and application server.
3. Enter the following command:

   ```
   cd %AUTOSYS%\dbobj\DataMover
   ```

   The DataMover directory appears.
4. Edit the following parameters in the paramfile file, using values based on your installation:

   SRCDBTYPE

   Defines the source database type. Valid values are *oracle*, *mssql*, 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.

   SRCDBPWD

   Defines the source database Unicenter AutoSys JM user password.

TGTDBTYPE

Defines the target database type. Valid values are *mssql*, *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 a Microsoft SQL Server, 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 Windows:**

  C:\Program Files\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.

5. Run the uajmdatamover.pl utility using the following command:

   ```
   perl uajmdatamover.pl paramfile
   ```

   A message appears if the verification test is successful.

6. Repeat Step 4, setting the VERIFY parameter to NO.

7. Repeat Step 5.

   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.

8. Start the scheduler using the CA Workload Automation AE Administrator, 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.

Appendix A: Removing CA Workload Automation AE

Uninstall CA Workload Automation AE

If necessary, you can uninstall CA Workload Automation AE using the installation wizard.

Important! Before uninstalling CA Workload Automation AE, stop all CA Workload Automation AE jobs or processes that are running on that computer. Otherwise, the uninstallation process may halt because the jobs or processes are still running. In that situation, you can wait until the jobs or processes complete, and click the Retry option on the Uninstall Complete page to continue the uninstallation. Alternatively, you can try to manually stop the processes by terminating the su.exe processes in the Windows Task Manager or by using a diagnostic tool.

To uninstall CA Workload Automation AE

1. Log in as a user with Windows Administrators group privileges.
2. Insert the installation media into the drive and mount it.

   Note: If autorun is enabled, the installation starts automatically.
3. Run setup.exe.

   The Product Explorer appears.
4. Select CA Workload Automation AE, and click Install.

   The Installation Wizard Welcome page appears.

   The Welcome page appears.
5. Select Remove and click Next.

   The Product Removal Selection page appears.
6. Select the Remove CA Workload Automation AE check box and click Next.

   The Review Settings page appears.
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 confirmation message appears.

8. Click Yes.

   The Setup Status page appears and the progress is displayed. When the update completes, the Uninstall Complete page appears.

9. Click Finish.

   The product is uninstalled.

Note: You can remove the database user and database files using the appropriate database utilities.

Index