CA Workload Automation AE

Release Notes

Release 11.3.6

CA Technologies Product References

This document references the following CA Technologies products:

- CA Automation Suite for Data Centers (formerly named CA Spectrum® Automation Manager)
- CA ControlMinder™ (formerly named CA eTrust® Access Control)
- CA Embedded Entitlements Manager (CA EEM)
- CA IT Client Manager
- CA Job Management Option
- CA Jobtrac™ Job Management (CA Jobtrac)
- CA Network and Systems Management (CA NSM)
- CA Process Automation
- CA Scheduler® Job Management (CA Scheduler)
- CA Service Desk
- CA Systems Performance for Infrastructure Managers (formerly named CA SystemEDGE)
- CA Universal Job Management Agent (CA UJMA)
- CA Workload Automation AE (formerly named Unicenter® AutoSys® Job Management (Unicenter AutoSys JM))
- CA Workload Automation AE Connect Option
- CA Workload Automation Agent for Application Services (CA WA Agent for Application Services)
- CA Workload Automation Agent for Databases (CA WA Agent for Databases)
- CA Workload Automation Agent for i5/OS (CA WA Agent for i5/OS)
- CA Workload Automation Agent for Linux (CA WA Agent for Linux)
- CA Workload Automation Agent for Micro Focus (CA WA Agent for Micro Focus)
- CA Workload Automation Agent for Oracle E-Business Suite (CA WA Agent for Oracle E-Business Suite)
- CA Workload Automation Agent for PeopleSoft (CA WA Agent for PeopleSoft)
- CA Workload Automation Agent for Remote Execution (CA WA Agent for Remote Execution)
- CA Workload Automation Agent for SAP (CA WA Agent for SAP)
- CA Workload Automation Agent for UNIX (CA WA Agent for UNIX)
- CA Workload Automation Agent for Web Services (CA WA Agent for Web Services)

- CA Workload Automation Agent for Windows (CA WA Agent for Windows)
- CA Workload Automation Agent for z/OS (CA WA Agent for z/OS)
- CA Workload Automation CA 7® Edition (formerly named CA Workload Automation SE)
- CA Workload Automation ESP Edition (formerly named CA Workload Automation EE)
- CA Workload Control Center (CA WCC)

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

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 5: Operating System and Database Support 41

Chapter 6: System Requirements 63

Chapter 7: Support for Other CA Technologies Products 69

Chapter 8: Related Documentation 77

Chapter 1: Welcome

Welcome to CA Workload Automation AE. This document describes feature and functionality enhancements for this release, supported operating systems and databases, system requirements, and known issues, if any.

For the latest version of the Release Notes, visit http://ca.com/support. For major releases, a full updated documentation set with a bookshelf is provided. You can find the bookshelf containing the Release Notes by searching the Find a Product Documentation Bookshelf section on the Documentation page.

Chapter 2: New Features

This chapter describes new features added to the product.

This section contains the following topics:

New Unauthenticated User Mode Setting

The EXTERNAL unauthenticated user mode setting enables you to authenticate client utilities using external authentication protocols when customized authentication libraries are installed on all client and server machines in the instance.

Note: For information about changing the unauthenticated user mode setting to EXTERNAL and about creating and installing customized authentication libraries, see the *Security Guide*.

Setting the Maximum Number of Lines to Retrieve from a Log File

You can set the maximum number of lines to retrieve from a log file.

On UNIX, you can configure this setting using the LogMaxEndLines parameter in the configuration file. For information about setting the maximum number of lines to retrieve from a log file on UNIX, see the *Administration Guide*.

On Windows, you can configure this setting using the Log Max End Lines field on the Application Server window of CA Workload Automation AE Administrator (autosysadmin). For information about setting the maximum number of lines to retrieve from a log file on Windows, see the *Online Help*.

Chapter 3: Changes to Existing Features

This chapter describes changes made to existing features and includes a list of any features removed from the product.

This section contains the following topics:

Authenticating Command Line Utilities with External Security

The addition of the -usr command line option enables you to authenticate certain command line utilities with external security. Using this option improves security by ensuring that the utility runs as an authenticated external security user.

The authentication of the external security user is successful only when the user's password is accurately specified using the -pw or -pwx parameter. When authentication fails, the utility does not run and exits with an error.

Following authentication, the external security system assigns a security policy identity to the utility. The security policy determines which protected CA Workload Automation AE objects are accessible based on the assigned identity and grants the utility access to those objects.

Notes:

■ This option is required when the CA Workload Automation AE instance is configured to run in external security mode and the unauthenticated user mode is set to STRICT; otherwise, it is optional.

■ The utility ignores this option when the CA Workload Automation AE instance is operating in native security mode.

■ For more information about which utilities support this option and how to use it, see the *Reference Guide*.

FORCE_STARTJOB (108)

In the current release, you can force start a job in FAILURE or TERMINATED status that has a virtual resource dependency with free=Y or free=N and has not released the virtual resources. The FORCE_STARTJOB event verifies if the job's current status is FAILURE or TERMINATED and schedules the job using the already held virtual resources.

Note: Before force starting the job, the scheduler does not re-evaluate other resource dependencies.

STARTJOB (107)

In the current release, you cannot issue the STARTJOB event to start a job that has a virtual resource dependency with free=Y or free=N and has already held the resource.

To start such a job, take *one* of the following actions:

■ Manually release the held resource by issuing the RELEASE_RESOURCE event.

■ Force start the job in FAILURE or TERMINATED status by issuing the FORCE_STARTJOB event. The virtual resource is released if the job has the virtual resource dependency with free=Y and completes successfully.

Note: For more information about the RELEASE_RESOURCE or FORCE_STARTJOB event, see the *Reference Guide*.

Updating the resource Attribute in an Existing Job Definition

You cannot update the resources attribute in the existing job definition if the job has a resource dependency and has held the resource.

To release the held resource, take *one* of the following actions:

■ Manually release the held resource by issuing the RELEASE_RESOURCE event.

■ Force start the job in FAILURE or TERMINATED status by issuing the FORCE_STARTJOB event. The virtual resource is released if the job has the virtual resource dependency with free=Y and completes successfully.

Note: For more information about the RELEASE_RESOURCE or FORCE_STARTJOB event, see the *Reference Guide*.

Documentation in the Product Image

The product documentation for future releases of CA Workload Automation AE will no longer be available in the product image. You can access the documentation online from CA Technologies approved websites.

Chapter 4: Known Issues

This chapter provides information about issues that are known to exist in this version.

Note: For information about agent limitations and known issues, see the *Readme* or *Release Notes* for your agent.

This section contains the following topics:

Agent Upgrade Fails (UNIX only)

If you are installing an agent using the wa_setup.sh script on a computer where the r11.3 agent is already installed, a message similar to the following is displayed:

```
There is already an agent installed with the name you specified. To
use the existing agent for this install, select Use an Existing
Agent. Otherwise, specify another agent name.
[ OK ] [ Abort installation ]
```

When you try to upgrade the agent from r11.3 to the current release using the wa_setup.sh script, the upgrade fails if the r11.3 agent was installed using the agent_setup.sh script. This happens because the Product Interchange Format (PIF) considers the agent_setup.sh and wa_setup.sh scripts as two different components.

To upgrade the agent from r11.3 to the current release successfully, you must use the same script that you used to install the r11.3 agent. For example, if you used the agent_setup.sh script to install the r11.3 agent, you must use the agent_setup.sh script to upgrade the agent from r11.3 to the current release.

Application Server Stops Responding (UNIX only)

If you installed CA Workload Automation AE on a UNIX computer, the application server may stop responding if the /etc/hosts file contains the ::1 entry (IPv6 loop back entry) that includes the host name. To resolve this issue, remove the host name from the ::1 entry in the /etc/hosts file.

CA Workload Automation AE Processes Fail to Start on Red Hat Linux Enterprise 6 (UNIX only)

CA Workload Automation AE processes exit with Signal SEGV error if the CA Workload Automation AE user does not have read and execute permissions to the $ORACLE_HOME directory. The CA Workload Automation AE processes exit without displaying any error messages.

As a workaround, the CA Workload Automation AE user must be granted read and execute permissions to the $ORACLE_HOME directory.

Database Connection Tests Issue During Installation (UNIX only)

During the CA Workload Automation AE installation, if the database connection tests take more than 90 seconds, the following message is displayed:

```
No further dialog defined — script returned no result.
```

To fix this issue, tune the network or the database such that the database connection test is performed within 90 seconds.

Database Creation Fails if the Database Server Resides on a Windows Computer (UNIX Only)

Symptom:

The CA Workload Automation AE installation fails to create the database if the database server resides on a Windows Computer, and the data file path contains special characters like \n, \t, and so on. For example, if you specify the data file path as C:\newdata, C:\tabdata, and so on.

Solution:

This problem occurs due to the UNIX/Linux shell interpretation of strings containing special characters.

To resolve this issue, do one of the following:

■ Do not use special characters in the data file path.

■ Specify the data file path as c://newdata, c://tabdata, and so on.

Default Shell on the Agent Must Be Bourne (UNIX Only)

When a job is submitted on a UNIX computer, the CA Workload Automation agent first processes the /etc/auto.profile file. This file is a Bourne shell script and is located on the agent computer. It sets the system environment variables for the job, including required variable definitions such as AUTOSYS.

Therefore, if you define jobs that run under an owner whose default login shell cannot run Bourne shell scripts (for example, the C shell), you must configure the default shell on the agent. Otherwise, you will get errors when the agent tries to run the /etc/auto.profile file, and your jobs will fail. By configuring the default shell, the agent overrides the login shell and runs the /etc/auto.profile file under the Bourne shell instead.

To configure the default shell on the agent, do the following:

1. On the UNIX computer where you want to run the job, change to the agent installation directory.

2. Stop the agent.

3. Open the agentparm.txt file.

4. Set the following parameters:

    oscomponent.defaultshell=/bin/sh
    oscomponent.defaultshell.force=true

5. Save and close the agentparm.txt file.

6. Start the agent.

    The agent uses the Bourne shell by default. When a job is submitted, the agent always runs the /etc/auto.profile under the Bourne shell to source the environment for the job.

Notes:

■   You can invoke any shell to run the script specified in the command attribute in a Command job. You can specify the shell in the first line of the script or you can add the shell attribute to the job definition. The agent invokes this shell after it runs the /etc/auto.profile file under the default Bourne shell.

■   For more information about the oscomponent.defaultshell and oscomponent.defaultshell.force parameters, see the *CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide*.

Defined Aliases (UNIX Only)

Defined aliases that change the native behavior of operating system commands can cause installation problems. Remove all defined aliases before installing CA Workload Automation AE.

Error Occurs When Running safex on SuSE and Solaris

An error can occur when you run the safex utility on SuSE (Linux) and Solaris (UNIX). To resolve this issue, verify or modify the following items in your configuration:

- On SuSE, include the following line in the LD_LIBRARY_PATH:

  CA_EEM_installation_location/lib

  Note: The default CA EEM installation location is /opt/CA/SharedComponents/EmbeddedEntitlementsManager.

- On Solaris, set the following environment variable:

  CAPKIHOME=*CAPKI_installation_location*

  Note: The default CAPKI installation location is /opt/CA/SharedComponents/CAPKI.

Insufficient Procedure Cache During Installation (UNIX Only)

The CA Workload Automation AE installation program may display warnings about insufficient procedure cache while creating a database. This problem occurs on UNIX platforms using a Sybase database. To prevent this problem, increase the procedure cache to 10000 KB before starting the CA Workload Automation AE installation.

Upgrading from 4.5.1 to the Current Release with CCISA Installed (UNIX only)

If you are upgrading from Unicenter AutoSys JM 4.5.1 to the current release and you have CCISA installed, you must specify the installation location of the CCISA component in the CA Shared Components input field during the CA Workload Automation AE Release 11.3.6 upgrade interview process. Otherwise, the upgrade will fail with the following errors:

```
ERROR: ca-cs-utils should be installed in /opt/CA/CCISA
Exiting..
!! Script executed with error: 1
Script or command "csutils/scripts/prein_csutils.sh" failed with exit code 1.
Reason:  The script or command encountered a problem.
Action:  Find further details in the installation log file.
```

To determine the install location of the CCISA component

1. Locate the CCISA install directory, which is found in the /opt/CA/.CCISAprodloc file. The default CCISA install location is /opt/CA/CCISA.

2. When you run the CA Workload Automation AE installation program to upgrade from 4.5.1, do the following:

    a. Select a Custom install.

    b. On the Installation Path panel, override the Shared Components directory default of /opt/CA/SharedComponents with the CCISA install directory located in Step 1.

Installation Does Not Proceed Further if the Installation Panels are Resized (UNIX only)

The CA Workload Automation AE installation does not proceed further if you resize the installation panels during the interview phase or during the installation. The installer displays an error message to abort the installation.

CAPKI in FIPS Mode (Linux only)

If you enable Security-Enhanced Linux (SELinux) feature on your computer, CAPKI cannot run in FIPS mode. To enable CAPKI to run in FIPS mode, you must disable the SELinux feature.

CA WCC May Not Validate CA Workload Automation AE User Credentials (HP-UX only)

On HP-UX, CA WCC may not be able to validate CA Workload Automation AE user credentials. To verify if this problem exists on your computer, run the following command from the agent installation directory:

```
chkusr root 059EA442581E1E7E8B0A
```

If a communication problem exists, the following error message appears:

```
chkusr root 059EA442581E1E7E8B0A
Unable to load pam library: Unable to find library 'libpam.sl'.
```

To resolve this problem, do the following:

1. (HPUX Itanium only) Create a symbolic link to the library named libpam:

   ```
   ln –s /usr/lib/hpux64/libpam.so /usr/lib/hpux64/libpam.sl
   ```

2. Set the library path:

   ■ On HP-UX PA-RISC, run the following commands:

   ```
   SHLIB_PATH=/usr/lib:$SHLIB_PATH
   export SHLIB_PATH
   ```

   ■ On HP-UX Itanium, run the following commands:

   ```
   SHLIB_PATH=/usr/lib/hpux64:$SHLIB_PATH
   export SHLIB_PATH
   ```

3. Enter the following command at the operating system prompt:

   ```
   unisrvcntr restart waae_agent-WA_AGENT
   ```

   WA_AGENT

   Defines the name of the agent to restart.

   The agent restarts.

4. Run the following command from the agent installation directory:

   ```
   chkusr root 059EA442581E1E7E8B0A
   ```

   If the communication is successful, the following message appears:

   ```
   chkusr root 059EA442581E1E7E8B0A
   User and Password okay
   ```

64-bit Windows Agent Cannot Communicate Using SSA Communication (Windows only)

If you install the agent on a Windows 64-bit computer using the CA Workload Automation Agent DVD and configure it to communicate using CA Secure Socket Adapter (SSA) communication, an error similar to the following is displayed when you start the agent:

```
- java.lang.UnsatisfiedLinkError: C:\Program Files (x86)\CA\SC\Csam\SockAdap
ter\bin\casocket_jni.dll: Can't load IA 32-bit .dll on a AMD 64-bit platform
```

This error occurs because SSA is a 32-bit application and the 64-bit Windows agent cannot communicate with a 32-bit SSA application.

To resolve this issue, you must reconfigure the agent to communicate using plain socket ports by setting the following parameters in the agentparm.txt file as follows:

```
communication.receiver.socket.main=plain
communication.inputport=port_number
```

port_number

> Specifies the non-SSA port number the agent uses to listen for incoming messages from CA Workload Automation AE.

Note: CA Workload Automation AE does not support blobs or globs in job definitions because the agent invokes the CA Workload Automation AE SDK, which uses SSA communication, to get the blob or glob information through the Application Server.

Application Server Not Starting Automatically (Windows only)

Even though the service is set to start automatically, the application server is not starting automatically after the product installation or server reboot. This happened only if the Oracle database listener was not up when the application server started.

As a workaround, restart the application server after the Oracle database listener is available and the normal operation is resumed.

CA EEM Error Message Appears in the Installation Log (Windows Only)

The following two sets of error messages appear in the installation log when you install CA Workload Automation AE and create CA EEM security policies for the instance:

```
CAUAJM_I_60318 Attempting connection to CA EEM Backend Server: xyz
CAUAJM_I_60231 Connection successful: xyz  User: EiamAdmin Application: Global
```
ERROR PozFactory - PozFactory::attachPoz - Error invoking iPoz::ClientAttach on host xyz
ERROR PozFactory - PozFactory::attachPoz Error: Could not match proxy to product instance

```
ConfigReader::readFileContent - unable to open eiam configuration file, config file
path=[C:\Program Files\CA\Workload Automation AE\autouser.ACE\eiam.client.config],
error message=[No such file or directory]
Safe::Configurator::init_internal : - error - unable to load configuration
```
ERROR: Safe::Configurator::term called without init
```
CAUAJM_I_60318 Attempting connection to CA EEM Backend Server: xyz
```

These messages result from the server trying to connect to an application instance on CA EEM that does not exist. The messages do not affect the working of the installation.

CA NSM JMO Dependent Jobs Not Running (Windows Only)

If a CA NSM JMO (CA Network and Systems Management Job Management Option) job name contains fewer than eight characters, CA NSM JMO does not send the RUNNING and SUCCESS job status to the CA Workload Automation AE instance. Therefore, the CA Workload Automation AE job that is dependent on the CA NSM JMO job does not run even if the CA NSM JMO job completes successfully.

Note: If you encounter this problem, contact CA Technical Support at http://ca.com/support for the latest patch.

Installation Fails (Windows only)

Symptom:

When I install CA Workload Automation AE on a computer where a CA Workload Automation AE instance is already installed from a mounted ISO drive or the DVD drive, the installation fails.

Solution:

Follow these steps:

1. Open regedit and browse for the following registry key:

   ```
   HKLM\Software\Classes\Installer\Products\D79FA0A0F351D8644BC9E030C2D3B00D\Sou
   rceList\Media
   ```

2. Add the MediaPackage string and set its value to EWA\AutoSys.

3. Install CA Workload Automation AE.

Note: For more information about this solution, refer to the Microsoft Knowledge Base article 299803.

Installing CA Workload Automation AE and CA WCC on the Same Computer (Windows only)

To install CA Workload Automation AE and CA WCC successfully on the same computer, you must install CA Workload Automation AE first and then install CA WCC. If you install CA Workload Automation AE on a computer where CA WCC is already installed, the installation fails.

To resolve this issue:

1. Locate the following registry entry:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserDa
   ta\S-1-5-18\Products\D79FA0A0F351D8644BC9E030C2D3B00D\InstallProperties
   ```

2. Edit the InstallSource key value by entering the CA Workload Automation AE installation msi path.

   Example: C:\WAAE114\EWA\AutoSys

3. Install CA Workload Automation AE.

Installation Fails on UAC Enabled Computers (Windows only)

CA Workload Automation AE fails to install on User Account Control (UAC) enabled computers. This happens because of UAC restrictions; a standard user from an administrator group does not have full privileges to install CA Workload Automation AE.

To install CA Workload Automation AE, follow these steps:

1. Right-click setup.exe.

2. Select "run as administrator" option.

3. Install CA Workload Automation AE.

Installer Does Not Set Up CA Workload Automation AE to Run in a High-Available Cluster Environment (Windows only)

When you install CA Workload Automation AE on Windows 2008 in a cluster environment, the installer is not able to set up CA Workload Automation AE to run in a highly-available cluster environment.

To set up CA Workload Automation AE to run in a highly-available cluster environment, do the following:

1. During the CA Workload Automation AE installation, clear the Configure this instance for a highly-available clustered environment check box on the Application Server Properties page, and continue with the installation.

    CA Workload Automation AE is installed without registering the instance for use in a cluster environment.

2. After you install CA Workload Automation AE, configure the application server and scheduler manually for use in a cluster environment.

    CA Workload Automation AE is set up to run in a highly-available cluster environment.

Register the Agent in CA IT Client Manager (Windows Only)

The itemproc.dat procedures file located at SDO\agent\reginfo is used to register procedures in the Software Delivery Manager component of CA IT Client Manager. Currently, this procedures file registers the CA Workload Automation AE agent in the Software Delivery Manager component of CA IT Client Manager.

As a workaround, when you install additional CA Workload Automation AE agents using the Software Delivery Manager component of CA IT Client Manager, you must modify the itemproc.dat procedures file to call the command as Setup.exe /s /f1"agent.iss".

For example, you can modify the following keywords in the itemproc.dat procedures file as follows:

```
Parameters = "/s /f1"C:\EWA\AutoSys\agent.iss""
ProcToRun = setup.exe
```

Set the Parameters keyword value to the path where the agent.iss file is located on the computer where the Software Delivery Manager component of CA IT Client Manager is installed.

Kuwait, Riyadh Time Zone May Display as Baghdad (Windows Only)

If you change the time zone on Windows to GMT +3:00 Kuwait, Riyadh and restart the CA Workload Automation AE scheduler, the scheduler log file shows the incorrect city as follows:

```
CAUAJM_I_40246 CA WAAE Scheduler startup complete
CAUAJM_I_40211 Using TZ = BAGHDAD
```

The scheduler displays the incorrect city because the Kuwait, Riyadh, and Baghdad time zones have the same Bias, Standard, and Daylight dates. The scheduler compares the time zone entries in the time zone .cfg file in the %AUTOSYS% directory with the TIME_ZONE_INFORMATION returned by the Windows API, GetTimeZoneInformation. Because the time zones have the same information, the scheduler reads the time zone that occurs first and displays it.

The information returned by the Windows API does not have any other information that identifies the city the Windows time zone is set to. Therefore, to work around this issue, do the following:

1. Open the time zone .cfg file in the %AUTOSYS% directory.

2. Move the <TZ="KUWAIT, RIYADH">...</TZ> entry to the beginning of the file.

3. Save the file.

4. Restart the scheduler.

The correct time zone is displayed.

testheart.exe Must Be Moved to %AUTOSYS%\bin (Windows Only)

A testheart.exe file is stored in the %AUTOSYS%\test\bin directory. Before running any jobs that may use the testheart.exe file, you must move testheart.exe to the %AUTOSYS%\bin directory. This is because CA Workload Automation AE Release 11.3.6 requires access to the Microsoft runtime manifest files located in %AUTOSYS%\bin.

Silent Installation Image Creation Failure (Windows only)

When you try to create the silent installation image of the agent, SDK, or the Oracle database scripts using the CA Workload Automation AE Product Explorer window from a shared network drive, the image creation fails.

To create the silent installation images of the agent, SDK, or the Oracle database scripts successfully, launch the CA Workload Automation AE Product Explorer window from a mapped drive or a local disk.

Upgrade Fails (Windows only)

Symptom:

When I upgrade CA Workload Automation AE r11.3 to the current release from a mounted ISO drive or the DVD drive, the upgrade fails.

Solution:

If you copy the installer from the mounted ISO drive to the local hard disk and perform the upgrade, the upgrade is successful. However, if you cannot copy the mounted ISO drive to the local hard disk or you upgrade using the DVD drive, follow these steps:

1. Open regedit and browse for the following registry key:

    ```
    HKLM\Software\Classes\Installer\Products\D79FA0A0F351D8644BC9E030C2D3B00D\Sou
    rceList\Media
    ```

2. Add the MediaPackage string and set its value to EWA\AutoSys.

3. Upgrade CA Workload Automation AE r11.3 to the current release.

Note: For more information about this solution, refer to the Microsoft Knowledge Base article 299803.

autobcpORA Script Completes With Warning Message (Oracle only)

On Oracle 11g Release 2, when you run the autobcpORA.pl script, the following warning message is displayed for all tables in the source database that do not have a single row inserted from the time they were created:

```
EXP-00011: AEDBADMIN.<Table Name> does not exist
```

This is the expected behavior and the autobcpORA script completes successfully.

Note: The warning message is displayed because the deferred_segment_creation parameter on the source database is enabled by default.

Datamover Fails to Validate Oracle Real Application Cluster (RAC) Database (Oracle only)

When you migrate data to an Oracle RAC database, the datamover utility fails to validate the database. This happens because you cannot connect to the Oracle RAC database using the JDBC thin client drivers.

As a workaround, you must run the datamover utility on individual nodes of the Oracle RAC database.

archive_jobs Command Does Not Delete All Logically Deleted Jobs

The archive_jobs command does not remove all jobs marked for deletion that meet the obsolete criteria as expected. In addition, the optional audit report produced using the -A option in the command may contain incomplete information or the message "CAUAJM_E_10257 Potential corruption of job data for joid <nnn>". The database is not corrupted; the CAUAJM_E_10257 message is a symptom of the jobs that were not completely deleted.

Application Server is Not Able to Connect to the Second CA EEM Host

If you configure CA Workload Automation AE to work with CA EEM that is running in high availability mode, the client utilities like forecast, autoaggr, or DBMaint fail if the itechpoz-router service on the primary CA EEM host is down and an error message similar to the following is displayed:

```
log4cxx: No appender could be found for logger (PozFactory).
log4cxx: Please initialize the log4cxx system properly.
CAUAJM_E_10436 Security server unreachable or invalid authentication certificate
file.
CAUAJM_E_10434 Error initiating security session.
CAUAJM_E_10437 Detailed Error Information:
[EE_NOTALLOWED Operation not allowed]
[attach to application instance not allowed]
CAUAJM_E_10433 Could not obtain security server from the database.
CAUAJM_E_10434 Error initiating security session.
```

This happens because CA EEM does not fail over to the second CA EEM host and the application server is not able to connect to the second CA EEM host.

As a workaround, you can do *one* of the following:

- Allow CA EEM failover to take place by either shutting down the primary CA EEM host (that is, the iGateway service is shut down) or taking the primary CA EEM host completely offline.

- Restart the primary CA EEM host.

Client Utilities Time Out When External Security is Enabled

When external security is enabled, client utilities (such as autorep) can time out. These timeouts happen when there are a large number of jobs to process and restrictive policies are specified in the as-job resource class.

fail_codes Attribute Does Not Work Properly

Currently fail_codes and success_codes attributes are mutually exclusive attributes; you cannot specify both attributes within a job definition. All non-zero exit codes are currently considered as a failure. To specify a non-zero exit code as a success, you must use the success_code attribute.

Note: These attributes only apply to Command and i5/OS job types.

Jobs Not Tracked When the Agent is Down

When CA Workload Automation Agent for UNIX, Linux, or Windows is down, the jobs that are currently running are not tracked. Therefore, when the agent restarts, CA Workload Automation AE cannot identify the state of the jobs that were running when the agent went down.

This issue only applies to jobs that are supported by the agent plug-ins, such as database, SAP, and PeopleSoft jobs. This issue does *not* apply to the following jobs:

- Command jobs
- File Trigger and File Watcher jobs
- FTP and Secure Copy jobs
- Monitoring Jobs

Lockout Issue after Installing CA Workload Automation AE

Installing CA Workload Automation AE on a computer where the autosys user account is not defined to the computer, but exists as a non-local account in an external user repository, may result in all users being locked out.

To prevent this problem, we recommend the following steps:

1. Install CA Workload Automation AE on machines where the autosys user account is defined locally.

2. If you install CA Workload Automation AE and you are locked out of autosys_secure, do *one* of the following:

   - Create a local account for "autosys" if you have the ability to add users to the computer. Logging onto the computer as the local "autosys" account should allow you to run autosys_secure as a super EDIT/EXEC user where you can add "autosys@host.networkdomain" as a EDIT/EXEC superuser. You can delete the local "autosys" account after completing this step.

   - Recreate the database by running the createnewdb Perl script located in %AUTOSYS%/dbobj or by running the CA Workload Automation AE installation. When the database is recreated, all the existing data in the database is lost.

Owner Attribute and user@host Value Must Match

The owner attribute and the user ID (user@host) defined in the database using autosys_secure are case-sensitive. When specifying the owner attribute in a job definition, the owner value must match the user@host value exactly, including case. Otherwise, the password associated with the owner cannot be retrieved.

Running SQL Transaction Cannot be Cancelled

If the transaction submitted by an SQL job is already running on the database server, the sendevent -E KILLJOB command does not cancel the transaction. CA Workload Automation Agent for UNIX, Linux, or Windows sends a confirmation to CA Workload Automation AE that the cancel request was submitted to the database server, but the transaction continues to run. The job goes to a SUCCESS state when the transaction is complete.

sap_job_count Attribute

If you run a job without specifying the sap_job_count attribute on an r11.3 SAP agent plug-in, the job fails. This happens because the sap_job_count attribute is required when you run a SAP Job Copy job on an agent with an r11.3 SAP agent plug-in.

Search in CA WCC Fails and Returns Database Errors

If you search non-object attributes (for example, job description) in CA WCC using the exclamation point character (!), the search fails and the CA Workload Automation AE API returns database errors.

sendevent Command Fails to the Lightweight Application Server

When you issue the sendevent command to the lightweight application server using the –S option, the command fails and an error message is displayed.

Notes:

- The –S option instructs the sendevent command to send an event to another instance other than the current instance. If the configuration for the other instance exists on the computer where the sendevent command is executed, the sendevent command contacts the application server corresponding to that instance.

- When you install an Release 11.3.6 application server and connect it to the event server used by an external 4.5.1 instance, that application server is named *lightweight application server*. The lightweight application server detects the presence of 4.5.1 event server data and runs with limited functionality. It processes external dependency and sendevent requests from the local Release 11.3.6 instance and writes job events directly into the 4.5.1 event server.

Update Job Fails with Multiple Machines

If you specify multiple machines in a job definition by separating each machine with a comma (,), the jil command fails to update the job with resource dependencies.

Web Services Login Failure

The web services experience login failures if the reverse DNS lookup returns the host name of the web services server with a different case than the hostname command. This problem occurs because CA EEM uses the host name as part of the encryption algorithm. For example, if the hostname command returns the host name as host.example.com with an IP address of 192.168.100.200 and nslookup 192.168.100.200 returns HOST.example.com, you experience this problem.

To solve this problem, ensure that the host name returned by the hostname command and the nslookup command using the IP address match exactly.

Command Sponsor Known Issues

This section contains known issues with the Command Sponsor.

JRE Not Removed During Command Sponsor Uninstallation (HP-UX Only)

When uninstalling the Command Sponsor on HP-UX, the JRE installed by the Command Sponsor is not completely removed. You can encounter problems reinstalling the Command Sponsor if the JRE is not removed.

The JRE must be removed manually by typing the following command in a console window:

```
"rm -rf $IGW_LOC/jre1.6.0_cs"
```

Cannot Execute CA Workload Automation AE Commands from CA WCC (HP-UX only)

On HP-UX, if you install the Command Sponsor component during the CA Workload Automation AE installation and configure CA WCC to work with CA Workload Automation AE, you cannot run some CA Workload Automation AE commands, such as chk_auto_up, from CA WCC.

An error similar to the following is displayed:

```
internal error has occurred
The command could not be executed. Command processing exception encountered.
```

As a workaround, you can do the following:

1. Comment the following line in the /etc/profile.igw file, as follows:

   ```
   #_JAVA_OPTIONS=-d32; export _JAVA_OPTIONS
   ```

2. Issue the following command:

   ```
   $IGW_LOC/S99igateway stop
   ```

   The iGateway service stops.

3. Issue the following command:

   ```
   $IGW_LOC/S99igateway start
   ```

   The iGateway service starts.

Note: The /etc/profile.igw file is created during CA EEM installation. Therefore, this problem only occurs if you install CA EEM after you install the Command Sponsor component.

Command Sponsor Fails to Install on Microsoft Windows (64-bit) Operating Systems

On all supported Microsoft Windows 64-bit operating systems, if you install the Command Sponsor on a computer on which the 64-bit version of iGateway is already installed using the CA Workload Automation AE DVD, a message similar to the following is displayed and the installation does not proceed further:

```
Command Sponsor supports only 32 bit version of iTechnology iGateway. The installation
has detected a 64 bit version of iTechnology iGateway and therefore cannot continue.
Exclude the Command Sponsor component to continue or uninstall the 64 bit version of
iTechnology iGateway.
```

To resolve this issue, uninstall the 64-bit version of iGateway and then install the Command Sponsor using the CA Workload Automation AE DVD.

Important! Verify that iGateway is not required by other installed software before you remove the 64-bit version.

Attempt to Get Job Log Fails

When checking the logs across the network using CA WCC, the following error message is displayed:

```
Failed to get the job log: CAUAJM_E_10673. The requested server operation failed.
Operation ID = 315
```

The Command Sponsor, which enables Enterprise Command Line and Reports functionality, runs on top of iGateway.

The following points apply to the iGateway port:

- The default port for iGateway 4.7.x is 5250. If you have configured iGateway to use a different port, verify that the port is open bidirectionally.

- If you are using iGateway with port 5250 and have restricted the port (for example, if you are using a firewall), verify that port 5250 is open bidirectionally.

Note: For information about configuring the iGateway port, see the iTech Development documentation.

Cannot Use CA Workload Automation AE Shell Alias

You cannot use a CA Workload Automation AE shell alias. For example, in Enterprise Command Line on UNIX, you cannot use se instead of sendevent.

The symptom is that the Command Sponsor does not work at all. When debugging, the igateway.log (in folder $IGW_LOC) contains an error that it could not load the JVM. This should occur only if the JRE referenced in igateway.conf in the <javahome> element is a 64-bit JRE. This can happen on AIX if the recommendation regarding the architecture of the JRE was not followed.

To resolve this issue, change the <javahome> element so that it points to a 32-bit JRE.

Cannot Import File Using CA WCC Enterprise Command Line

On UNIX, a file import using Enterprise Command Line can fail because of an incorrect unmask value in an environment setting.

To set the correct unmask value, follow these steps:

1. Run the following command:

   $IGW_LOC/S99igateway stop

2. Open the file at the following location:

   $IGW_LOC/S99igateway

3. Insert the following command on the line preceding the line that contains ./igateway –b:

   unmask 022

4. Insert the following command on the line preceding the line that contains ./igateway –d:

   unmask 022

5. Save the file.

6. Run the following command:

   `$IGW_LOC/S99igateway start`

Chapter 5: Operating System and Database Support

CA supports the subsequent operating systems for the duration of their life cycle (as determined by the operating system's manufacturer or until CA announces that we are dropping support). The supported operating systems are subject to change. For more information about compatibility and to see the latest operating systems supported, visit http://ca.com/support.

Notes:

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

■   The term *Windows* refers to any Microsoft Windows operating system supported by CA Workload Automation AE unless otherwise noted.

This section contains the following topics:

Server Supported Versions

UNIX

The CA Workload Automation AE server component supports the following UNIX versions:

Operating Environment	Supported Versions	Architecture	Notes
AIX	6.1	64-bit	The AIX C++ Runtime Environment must be at level 11.1.0.0 or higher. To see what level your system is at, run: lslpp -l xlC.aix50.rte
AIX	7.1	64-bit	The AIX C++ Runtime Environment must be at level 11.1.0.0 or higher. To see what level your system is at, run: lslpp -l xlC.aix50.rte

Operating Environment	Supported Versions	Architecture	Notes
HP-UX	11i v3 (11.31)	IA 64-bit (Itanium) PA-RISC 64-bit	
Solaris	10	SPARC 64-bit	Global zone and non-global whole/sparse root zone configurations are supported. You must install the following patch: 119963-04 SunOS 5.10: Shared library patch for C++ Nov/30/2005
Solaris	11	SPARC 64-bit	Global zone and non-global whole/sparse root zone configurations are supported.

Linux

The CA Workload Automation AE server component supports the following Linux versions:

Operating Environment	Supported Versions	Architecture	Notes
Oracle Enterprise Linux	5	x86 32/64bit	compat-libstdc++-33 or higher is required. The 32-bit version is required on the 64-bit version of Linux. libstdc++.so.5 and libstdc++.so.6 or higher are required. The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package. The libstdc++.so.6 shared library is contained in the libstdc++ rpm package. libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux. libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux. Perl version 5.8 or higher is required. ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux. glibc 2.4 (32-bit) or higher is required.

Operating Environment	Supported Versions	Architecture	Notes
Oracle Enterprise Linux	6	x86 32/64bit	compat-libstdc++-33 or higher is required. The 32-bit version is required on the 64-bit version of Linux.
			libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
			libgcc-4.4 (32-bit) or higher is required.
			nss-softokn-freebl-3.12 (32-bit) or higher is required.
			The following rpm packages are required on the 64-bit version of Linux:
			■ audit-libs-2.0.4-1.el6.i686.rpm
			■ cracklib-2.8.16-2.el6.i686.rpm
			■ pam_passwdqc-1.0.5-6.el6.i686.rpm
			■ pam_ldap-185-5.el6.i686.rpm
			■ pam_krb5-2.3.11-1.el6.i686.rpm
			■ pam-1.1.1-10.el6_2.1.i686.rpm

Operating Environment	Supported Versions	Architecture	Notes
Red Hat Enterprise Linux	5	x86 32/64-bit	compat-libstdc++-33 or higher is required. The 32-bit version is required on the 64-bit version of Linux.
			libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.

Operating Environment	Supported Versions	Architecture	Notes
Red Hat Enterprise Linux	6	x86 32/64-bit	compat-libstdc++-33 or higher is required. The 32-bit version is required on the 64-bit version of Linux.
			libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
			libgcc-4.4 (32-bit) or higher is required.
			nss-softokn-freebl-3.12 (32-bit) or higher is required.
			The following rpm packages are required on the 64-bit version of Linux:
			■ audit-libs-2.0.4-1.el6.i686.rpm
			■ cracklib-2.8.16-2.el6.i686.rpm
			■ pam_passwdqc-1.0.5-6.el6.i686.rpm
			■ pam_ldap-185-5.el6.i686.rpm
			■ pam_krb5-2.3.11-1.el6.i686.rpm
			■ pam-1.1.1-10.el6_2.1.i686.rpm

Operating Environment	Supported Versions	Architecture	Notes
SuSE Linux Enterprise Server	10	x86 32/64-bit	The 32-bit versions of libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ or libstdc++-33 rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
			glibc-locale-32bit rpm package is required.
SuSE Linux Enterprise Server	11	x86 32/64-bit	The 32-bit versions of libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the libstdc++-33 rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
			glibc-locale-32bit rpm package is required.
Red Hat Cluster Suite			

Notes:

■ The Command Sponsor, installed using the CA Workload Automation AE DVD, enables support for the CA WCC Enterprise Command Line and Forecast applications. On Linux, the Command Sponsor supports only kernel version 2.6.

■ If the iGateway built on Linux 2.4 kernel version is already installed, then CA EEM, iGateway and all other iGateway plug-ins, and the Command Sponsor cannot be installed or upgraded. If $IGW_LOC/igw.linux_k26 file is present, then the iGateway built on Linux 2.6 kernel version is installed. In the case where the iGateway built on Linux 2.4 kernel version is already installed, uninstall CA EEM, iGateway and all other iGateway plug-ins, and the Command Sponsor, and then install these products using the CA Workload Automation AE DVD or the CA Common Components DVD. CA EEM policies can then be migrated to the new CA EEM installation. For information about migrating CA EEM policies, see the *CA Workload Automation Security Guide*. For more information about how to uninstall and install the Command Sponsor, see the *UNIX Implementation Guide*.

■ The glibc-locale-32bit rpm package is required to initialize the CA EEM SDK properly. For more information about CA EEM SDK initialization, see the *CA Embedded Entitlements Manager Programming Guide*.

Windows

The CA Workload Automation AE server component supports the following Windows versions:

Version	Architecture	Notes
Microsoft Windows 2008	x86 32/64-bit	Windows patch 979306 is required.
Microsoft Windows 2008 R2	x86 64-bit	Windows patch 979306 is required.
Microsoft Windows 2012	x86 64-bit	Windows patch 979306 is required.
Microsoft Cluster Server		

Client and SDK Supported Versions

UNIX

The CA Workload Automation AE client and SDK components support the following UNIX versions:

Operating Environment	Supported Versions	Architecture	Notes
AIX	6.1	64-bit	The AIX C++ Runtime Environment must be at level 11.1.0.0 or higher. To see what level your system is at, run: lslpp -l xlC.aix50.rte
AIX	7.1	64-bit	The AIX C++ Runtime Environment must be at level 11.1.0.0 or higher. To see what level your system is at, run: lslpp -l xlC.aix50.rte
HP-UX	11i v3 (11.31)	IA 64-bit (Itanium) PA-RISC 64-bit	
Solaris	10	SPARC 64-bit	Global zone and non-global whole/sparse root zone configurations are supported. You must install the following patch: 119963-04 SunOS 5.10: Shared library patch for C++ Nov/30/2005
Solaris	11	SPARC 64-bit	Global zone and non-global whole/sparse root zone configurations are supported.

Linux

The CA Workload Automation AE client and SDK components support the following Linux versions:

Operating Environment	Supported Versions	Architecture	Notes
Red Hat Enterprise Linux	5	x86 32/64-bit	compat-libstdc++-33 or higher is required. The 32-bit version is required on the 64-bit version of Linux.
			libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.

Operating Environment	Supported Versions	Architecture	Notes
Red Hat Enterprise Linux	6	x86 32/64-bit	compat-libstdc++-33 or higher is required. The 32-bit version is required on the 64-bit version of Linux.
			libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
			libgcc-4.4 (32-bit) or higher is required.
			nss-softokn-freebl-3.12 (32-bit) or higher is required.
			The following rpm packages are required on the 64-bit version of Linux:
			■ audit-libs-2.0.4-1.el6.i686.rpm
			■ cracklib-2.8.16-2.el6.i686.rpm
			■ pam_passwdqc-1.0.5-6.el6.i686.rpm
			■ pam_ldap-185-5.el6.i686.rpm
			■ pam_krb5-2.3.11-1.el6.i686.rpm
			■ pam-1.1.1-10.el6_2.1.i686.rpm

Operating Environment	Supported Versions	Architecture	Notes
SuSE Linux Enterprise Server	10	x86 32/64-bit	The 32-bit versions of libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ or libstdc++-33 rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
			glibc-locale-32bit rpm package is required.
SuSE Linux Enterprise Server	11	x86 32/64-bit	The 32-bit versions of libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the libstdc++-33 rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
			glibc-locale-32bit rpm package is required.

Note: The glibc-locale-32bit rpm package is required to initialize the CA EEM SDK properly. For more information about CA EEM SDK initialization, see the *CA Embedded Entitlements Manager Programming Guide*.

Windows

The CA Workload Automation AE client and SDK components support the following Windows versions:

Version	Architecture	Notes
Microsoft Windows 2008	x86 32/64-bit	Windows patch 979306 is required.
Microsoft Windows 2008 R2	x86 64-bit	Windows patch 979306 is required.
Microsoft Windows XP SP2 Professional	x86 32/64-bit	Windows patch 979306 is required.
Microsoft Windows Vista	x86 32/64-bit	Windows patch 979306 is required.
Microsoft Windows 7	x86 32/64-bit	Windows patch 979306 is required.
Microsoft Windows 2012	x86 64-bit	Windows patch 979306 is required.

Agent Supported Versions

Notes:

- If you install the agent on an operating system where the native CA Workload Automation AE client is not installed, you cannot issue the autoping command with the -S option or run jobs that contain globs or blobs as input or output.

- If you install the 64-bit agent using the CA Workload Automation Agent for UNIX, Linux, or Windows DVD, you cannot issue the autoping command with the -S option or run jobs that contain globs or blobs as input or output. The native CA Workload Automation AE client or SDK runs only in 32-bit mode and does not support being called by a 64-bit application.

- If you install the 32-bit agent using the CA Workload Automation Agent for UNIX, Linux, or Windows DVD, you cannot issue the autoping command with the -S option or run jobs that contain globs or blobs as input or output on operating systems that are not supported by the CA Workload Automation AE agent.

UNIX

The CA Workload Automation AE agent component supports the following UNIX versions:

Operating Environment	Supported Versions	Architecture	Notes
AIX	5.3	32/64-bit	

Operating Environment	Supported Versions	Architecture	Notes
AIX	6.1	64-bit	You must install the latest fix pack from the IBM website. You can download the patch from http://www-933.ibm.com/support/fixcentral.
AIX	7.1	64-bit	You must install the latest fix pack from the IBM website. You can download the patch from http://www-933.ibm.com/support/fixcentral.
HP-UX	11i v1 (11.11)	PA-RISC 32/64-bit	
HP-UX	11i v2 (11.23)	IA 64-bit (Itanium) PA-RISC 32/64-bit	On HP-UX PA-RISC computers, install the required patches as follows: ■ HP-UX 11i v1 (11.11) PA-RISC—PHSS_35385 ■ HP-UX 11i v2 (11.23) PA-RISC—PHSS_37201 ■ HP-UX 11i v3 (11.31) PA-RISC—PHSS_37202
HP-UX	11i v3 (11.31)	IA 64-bit (Itanium) PA-RISC 32/64-bit	
Solaris	9	SPARC 32/64-bit	
Solaris	10	SPARC 32/64-bit x86 32/64-bit	You must use the CA Workload Automation Agent for UNIX, Linux, or Windows DVD to install the agent on a Solaris x86 32/64-bit computer. 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*. Global zone and non-global whole/sparse root zone configurations are supported.
Solaris	11	SPARC 32/64-bit x86 32/64-bit	You must use the CA Workload Automation Agent for UNIX, Linux, or Windows DVD to install the agent on a Solaris x86 32/64-bit computer. 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*. Global zone and non-global whole/sparse root zone configurations are supported.

Linux

The CA Workload Automation AE agent component supports the following Linux versions:

Operating Environment	Supported Versions	Architecture	Notes
Red Hat Enterprise Linux	4	x86 32/64-bit	compat-libstdc++-33 or higher package (RPM) is required that supports GLIBCXX_3.2.3 or higher. The 32-bit version is required on the 64-bit version of Linux.
			libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.

Operating Environment	Supported Versions	Architecture	Notes
Red Hat Enterprise Linux	5	x86 32/64-bit	compat-libstdc++-33 or higher package (RPM) is required that supports GLIBCXX_3.2.3 or higher. The 32-bit version is required on the 64-bit version of Linux.
			libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.

Operating Environment	Supported Versions	Architecture	Notes
Red Hat Enterprise Linux	6	x86 32/64-bit	compat-libstdc++-33 or higher is required. The 32-bit version is required on the 64-bit version of Linux.
			libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
			libgcc-4.4 (32-bit) or higher is required.
			nss-softokn-freebl-3.12 (32-bit) or higher is required.
			The following rpm packages are required on the 64-bit version of Linux:
			■ audit-libs-2.0.4-1.el6.i686.rpm
			■ cracklib-2.8.16-2.el6.i686.rpm
			■ pam_passwdqc-1.0.5-6.el6.i686.rpm
			■ pam_ldap-185-5.el6.i686.rpm
			■ pam_krb5-2.3.11-1.el6.i686.rpm
			■ pam-1.1.1-10.el6_2.1.i686.rpm

Operating Environment	Supported Versions	Architecture	Notes
SuSE Linux Enterprise Server	9	x86 32/64-bit	The 32-bit versions of libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ or libstdc++-33 rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.
SuSE Linux Enterprise Server	10	x86 32/64-bit	The 32-bit versions of libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the compat-libstdc++ or libstdc++-33 rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.

Operating Environment	Supported Versions	Architecture	Notes
SuSE Linux Enterprise Server	11	x86 32/64-bit	The 32-bit versions of libstdc++.so.5 and libstdc++.so.6 or higher are required.
			The libstdc++.so.5 shared library is contained in the libstdc++-33 rpm package.
			The libstdc++.so.6 shared library is contained in the libstdc++ rpm package.
			libuuid.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			libaio.so.1 is required. The 32-bit version is required on the 64-bit version of Linux.
			Perl version 5.8 or higher is required.
			ncurses (32-bit) version 5 or higher is required on the 64-bit version of Linux.
			glibc 2.4 (32-bit) or higher is required.

Windows

The CA Workload Automation AE agent component supports the following Windows versions:

Version	Architecture
Microsoft Windows 2003 R2	x86 32/64-bit
Microsoft Windows 2003 SP1	x86 32/64-bit
Microsoft Windows 2008	x86 32/64-bit
Microsoft Windows 2008 R2 SP2	x86 64-bit
Microsoft Windows XP SP3 Professional	x86 32/64-bit
Microsoft Windows Vista	x86 32/64-bit
Microsoft Windows 7	x86 32/64-bit
Microsoft Windows 8	x86 32/64-bit
Microsoft Windows 2012	x86 64-bit

Database Support

CA Workload Automation AE supports the following databases:

Database	Supported Versions	Architecture	Notes
Microsoft SQL Server	2008	32/64-bit	
Microsoft SQL Server	2008 R2	32/64-bit	
Microsoft SQL Server	2012	32/64-bit	
Oracle	10g	32/64-bit RAC	10g R2 is supported. Oracle 10g patches are required to address SGA memory leaks and Oracle connectivity problems. For more information, see Oracle 10g Patches (see page 60).
Oracle	11g	32/64-bit RAC	11g R2 is supported.
Sybase ASE	15.0	32/64-bit	15.0.x, 15.5, and 15.7 are supported. The minimum page size must be at least 4 KB. Up to 137 free Sybase user connections are required, depending on which CA Workload Automation AE components you install. Sybase jConnect 7 is required. For more information about installing Sybase jConnect 7, contact your database vendor.

Important! To use the 64-bit version of an Oracle or Sybase database, you must install the 32-bit client if it is not already installed, and modify the path or library path environment variable. Complete these procedures before installing CA Workload Automation AE.

For HP-UX Itanium (IA-64) support, install the 32-bit HP-UX PA-RISC Oracle or Sybase client.

For instructions on configuring the environment to use a 64-bit database, see the *UNIX Implementation Guide* and *Windows Implementation Guide*.

Note: For more information about database configuration tasks and database migrations, see the *UNIX Implementation Guide* and *Windows Implementation Guide*.

Oracle 10g Patches

If you are installing CA Workload Automation AE Release 11.3.6 to work with Oracle 10g, you must install the appropriate Oracle patch to address the following issues:

SGA Memory Leaks in Oracle 10g Release 1

If you choose Oracle 10g Release 1 as the database for installing CA Workload Automation AE Release 11.3.6, you must apply Oracle 10g Release 1, Patch Set 5 (10.1.0.5) or higher to avoid SGA memory leaks while running CA Workload Automation AE Release 11.3.6 for extended periods.

If you do not apply this patch, you might get "ORA-04031 errors" and "CAUAJM_E_00051 Unable to create thread!" messages in the scheduler or application server log files.

Oracle Connectivity Problem When %AUTOSYS% Contains Special Characters on Windows

If the CA Workload Automation AE installation path (for example, %AUTOSYS%) contains special characters (for example, parentheses or quotation marks), you will get connectivity problems with the Oracle database. This is an Oracle problem. See Oracle BUG #3807408.

If you are using an Oracle version not mentioned in this document, contact Oracle support to obtain the necessary patches for your environment. See below for release/patch information.

Description of Oracle BUG #3807408:

Externally authenticated usernames containing a '(',')' or '=' cannot be authenticated, additionally if a program name / path contains these characters, it may not be possible to connect (ORA-12154).

For Oracle 10g on Windows, download and apply the following patches, as appropriate:

- 10.2.0.2:

    32-bit patch 5383042

    64-bit (Itanium) patch 5388866

    64-bit (x64) patch 5388871

- 10.2.0.1:

    32-bit patch 4923768

    64-bit (Itanium) patch 4923780

    64-bit (x64) patch 4923787

Patch 979306—Time Zone Update for Windows

For CA Workload Automation AE to work correctly with daylight saving time (DST), you must install patch 979306 on the CA Workload Automation AE client computers.

You can download the patch from http://support.microsoft.com/kb/955839.

For more information about configuring DST for Windows, see http://support.microsoft.com/kb/914387.

Note: The patch number is 979306 at the time of General Availability (GA). This patch may be superseded post GA. Ensure that you install the latest patch. For current information about time zone patches, check the Microsoft Support web site.

Chapter 6: System Requirements

This chapter describes the system requirements for CA Workload Automation AE.

This section contains the following topics:

System Requirements for UNIX and Linux

Note: As the number of users and the workload increases, you may see a performance benefit from adding additional memory and/or additional processing power. Additional processing power can be added either by using a faster CPU or by adding additional CPUs.

To install and run the CA Workload Automation AE server in a UNIX or Linux environment, the minimum recommended requirements are as follows:

- Processor: 1 GHz, 2CPU

- Physical memory: 4 GB RAM

- Swap space: 2 GB

- Hard disk free space: 5 GB

- fsize: The file size ulimit must be set to unlimited. To determine the current setting, issue the following command:

  ```
  ulimit -f
  ```

  If the value is not unlimited, change this ulimit value by issuing the following command:

  ```
  ulimit -f unlimited
  ```

- Disk space requirements for CA Workload Automation AE:

    - Full product: 700 MB

    - Application Server, Client, Command Sponsor: 520 MB

    - Scheduler, Client, Agent: 430 MB

    - Application Server, Web Server: 360 MB

    - Application Server only: 300 MB

    - Agent only: 420 MB

    - Client only: 300 MB

    - SDK only: 250 MB

    - Documentation only: 250 MB

    Notes:

    - The system temporary directory (/tmp or $TMPDIR) requires a minimum of 400 MB disk space for the installation.

    - The installer creates a directory to store control files. By default, the /opt/CA/installer directory is created. The file system that the installer directory belongs to requires a minimum of 10 MB disk space. For more information about the /opt/CA/installer directory, see the *CA Workload Automation AE UNIX Implementation Guide*.

- SDK runtime environment: 250 MB

- Disk space for the database (to support default installation values):

    - Oracle: Data—800 MB, Index—80 MB

    - Sybase: Data—800 MB, Log—100 MB, tempdb—500 MB, tempdb log—50 MB

    Note: For more information about the database requirements, see the appropriate database documentation or consult your database administrator. For information about tuning the database, see the *Administration Guide*.

System Requirements for Windows

Note: As the number of users and the workload increases, you may see a performance benefit from adding additional memory and/or additional processing power. Additional processing power can be added either by using a faster CPU or by adding additional CPUs.

To install and run the CA Workload Automation AE server in a Windows environment, the minimum recommended requirements are as follows:

- Processor: 2 GHz, 2CPU

- Physical memory: 4GB RAM

- Swap file: 2GB

- Hard disk free space: 5 GB

- Disk space requirements for CA Workload Automation AE:

  - Full product: 630 MB

  - Application Server, Client, Command Sponsor: 430 MB

  - Scheduler, Client, Agent: 310 MB

  - Application Server, Web Server: 350 MB

  - Application Server only: 180 MB

  - Agent only: 290 MB

  - Client only: 180 MB

  - SDK only: 40 MB

  - Documentation only: 40 MB

- SDK runtime environment: 50 MB

- Disk space requirements for the database (to support default installation values):

  - Microsoft SQL Server: 40 MB plus 1 MB for log file

    Note: SQL Server adjusts the sizes incrementally over time based on usage.

  - Oracle: Data—800 MB, Index—80 MB

  - Sybase: Data—800 MB, Log—100 MB, tempdb—500 MB, tempdb log—50 MB

Note: For more information about the database requirements, see the appropriate database documentation or consult your database administrator. For information about tuning the database, see the *Administration Guide*.

Java Runtime Environment (JRE) Supported Versions

The JRE is automatically installed with CA Workload Automation AE. The supported JRE versions are as follows:

Operating Environment	Supported JRE Version
AIX	1.7.0_04
HP-UX	1.6.0_17
Linux	1.7.0_17
Solaris	1.7.0_17
Windows	1.7.0_17

Notes:

- The supported JRE for all CA Workload Automation AE components is 32-bit. The only exception is the web server component, which supports only the 64-bit JRE.

- On a 64-bit computer, if you select to install the web server component during the CA Workload Automation AE installation, the 64-bit JRE is installed along with the web server.

- On HP-UX, when you run Java programs that use the CA Workload Automation AE Java SDK, run with the -V2 parameter. On HP-UX Itanium (IA-64), use the -pa20 argument with the -V2 parameter.

TCP/IP Port Usage

CA Workload Automation AE uses SSA for communication, which uses IANA assigned port 7163. SSA is automatically installed with CA Workload Automation AE.

By default, the CA Workload Automation AE communication with the agent is set up to use plain socket communication. The agent's default port number is 7520.

su Command on UNIX

On UNIX, the CA Workload Automation AE installer must be allowed to run the following command with no user response or interaction:

```
su – root –c "command"
```

The installer embeds other installation packages that are executed by running the su command.

Graphical Mode Requirements for UNIX and Linux

Before you install CA Workload Automation AE on UNIX or Linux, verify the following requirements are met so that installation dialogs can appear in graphical mode:

- Java 1.3 or higher is installed, the PATH environment variable is set to include the Java executable, and the JAVA_HOME environment variable is set.

- The monitor is graphics-enabled.

Base Application Development Math Library Package for AIX

Before you install CA Workload Automation AE on AIX, verify the system has the Base Application Development Math Library package (bos.adt.libm). The CA Workload Automation AE application server and the scheduler installations require this package.

User Resource Limits for AIX 64-bit

To install and run CA Workload Automation AE on AIX, verify the following variable=value pairs exist in /etc/security/limits for a 64-bit installation:

```
default:
fsize = -1
core = 2097151
cpu = -1
data = -1
rss = -1
stack = 262144
nofiles = 4096
```

You must restart the computer for the changes to take effect and before starting the installation.

HP-UX Itanium Processor

To install CA Workload Automation AE in an HP-UX Itanium environment, the kernel tunable parameter pa_maxssiz_32bit must be set to 268435456 or greater.

To view the current value of the pa_maxssiz_32bit parameter, enter the following command at the operating system prompt:

`/usr/sbin/kctune | grep pa_maxssiz_32bit`

To change the value of the pa_maxssiz_32bit parameter, do the following:

1. Enter the following command at the operating system prompt:

   `/usr/sbin/kctune pa_maxssiz_32bit=268435456`

2. Restart the computer.

   The pa_maxssiz_32bit parameter is set to the minimum required value.

Perl

On UNIX or Linux installations, Perl, version 5.8 or greater must be installed. Perl must also be included in the PATH environment variable to run the CA Workload Automation AE installation.

Chapter 7: Support for Other CA Technologies Products

This chapter describes other CA Technologies products supported by CA Workload Automation AE.

This section contains the following topics:

Location of CA License Files

The CA Workload Automation AE installer for Windows creates the following directory to store license files:

system_drive:\Program Files\CA\SharedComponents\CA_LIC

system_drive

Specifies the Windows operating system drive of the CA Workload Automation AE scheduler. This value is assigned automatically. You cannot change this drive or path even if other CA components are installed on a different drive. The CA licensing program shared by CA software does not support the customization of this path.

Note: On UNIX systems, the location of the license files depends on the value set by the CASHCOMP environment variable.

CA EEM Support

CA Workload Automation AE supports CA EEM Release 12.51. CA EEM includes the following features:

- Scalability

- Event Management and Persistence

- Reliable Event Delivery

- Authentication

You can install CA EEM using the CA Common Components DVD.

Notes:

- If the iGateway built on Linux 2.4 kernel version is already installed, CA EEM, iGateway, and all other iGateway plug-ins cannot be installed or upgraded. If $IGW_LOC/igw.linux_k26 file is present, then the iGateway built on Linux 2.6 kernel version is installed. In the case where the iGateway built on Linux 2.4 kernel version is already installed, uninstall CA EEM, iGateway, and all other iGateway plug-ins, and then install these products using the CA Common Components DVD. CA EEM policies can then be migrated to the new CA EEM installation. For information about migrating CA EEM policies, see the *CA Workload Automation Security Guide*. For information about upgrading CA EEM see the *CA Embedded Entitlements Manager Implementation Guide*.

- For more information about installing CA EEM, see the CA Common Components documentation.

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

- For more information about CA EEM features, see the CA EEM documentation.

CA Workload Automation AE, CA WCC, and CA EEM Compatibility

Requirements for compatibility between CA Workload Automation AE, CA WCC, and CA EEM depend on the security configuration of the products.

The following table displays the releases of CA Workload Automation AE, CA WCC, and CA EEM that are compatible:

CA WCC Release	CA Workload Automation AE Release	CA EEM Release
Release 11.3.6 (running in non-FIPS mode)	Release 11.3.6 (running in non-FIPS mode)	Release 12.51 (running in non-FIPS mode)

CA WCC Release	CA Workload Automation AE Release	CA EEM Release
Release 11.3.6 (running in non-FIPS mode)	Release 11.3.5 (running in non-FIPS mode) **Note:** We do not recommend this configuration as CA Workload Automation AE Release 11.3.5 does not necessarily contain all maintenance.	Release 12.51 (running in non-FIPS mode)
Release 11.3.6 (running in non-FIPS mode)	r11.3 SP1	Release 12.51 (running in non-FIPS mode)
Release 11.3.6 (running in FIPS mode)	Release 11.3.6 (running in FIPS mode)	Release 12.51 (running in FIPS mode)
Release 11.3.6 (running in FIPS mode)	Release 11.3.5 (running in FIPS mode) **Note:** We do not recommend this configuration as CA Workload Automation AE Release 11.3.5 does not necessarily contain all maintenance.	Release 12.51 (running in FIPS mode)

Notes:

- In external security mode, CA Workload Automation AE r11.3 and r11.3 SP1 use CA EEM r8.4 SDK libraries to connect to CA EEM r8.4. These libraries also support interactions with CA EEM Release 12.51 running in non-FIPS mode. To run CA WCC Release 11.3.6 in non-FIPS mode with CA Workload Automation AE r11.3 SP1, upgrade to CA EEM Release 12.51 and verify that CA EEM is running in non-FIPS mode. For information about CA EEM, see the *CA Embedded Entitlements Manager Implementation Guide.*

- In external security mode, CA Workload Automation AE Release 11.3.5 uses CA EEM Release 12.0 SDK libraries to connect to CA EEM Release 12.0. To run CA WCC Release 11.3.6 in FIPS mode with CA Workload Automation AE Release 11.3.5 in FIPS mode, verify that CA EEM is running in FIPS mode. However, for these products to be compatible with each other, we recommend that you take the following actions:

  - Upgrade CA WCC to Release 11.3.6

  - Upgrade CA Workload Automation AE to Release 11.3.6

  - Upgrade CA EEM to Release 12.51 and verify that CA EEM is running in FIPS mode.

- If you install CA WCC Release 11.3.6 on a computer where CA Workload Automation AE is installed, CA Workload Automation AE must also be Release 11.3.6.

- CA Workload Automation Agent for UNIX, Linux, or Windows can be installed on the same server with CA WCC Release 11.3.6 if the agent is installed using the CA Workload Automation AE Release 11.3.6 DVD. On UNIX, you can also install the agent using the CA Workload Automation AE Release 11.3.6 Standalone Agent DVD. Before you install the agent, stop the CA WCC services.

- On UNIX, if you want to install CA Workload Automation AE Release 11.3.6 on a computer where CA WCC Release 11.3.6 is already installed, you must stop the CA WCC services before you install CA Workload Automation AE Release 11.3.6.

- On Windows, to install CA Workload Automation AE and CA WCC successfully on the same computer, you must install CA Workload Automation AE first and then install CA WCC. If you install CA Workload Automation AE on a computer where CA WCC is already installed, the installation fails. To resolve this issue, see Installing CA Workload Automation AE and CA WCC on the Same Computer (see page 27).

CA Secure Socket Adapter Support

CA Workload Automation AE supports 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 is installed automatically during the CA Workload Automation AE installation.

Notes: For more information about configuring port numbers and settings, see the *CA Workload Automation AE UNIX Implementation Guide* or *Windows Implementation Guide*.

CA Automation Suite for Data Centers Support

CA Workload Automation AE works with CA Automation Suite for Data Centers for load balancing and scheduling based on real-time resource utilization. To integrate with CA Workload Automation AE, CA Automation Suite for Data Centers r12 SP1 or higher and its SDK client are required.

Note: For more information about configuring CA Workload Automation AE to work with CA Automation Suite for Data Centers, see the *UNIX Implementation Guide* or *Windows Implementation Guide*.

Notification Services Support

Valid on Windows only

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

To integrate CA Workload Automation AE with Notification Services, you must install Notification Services from CA NSM r11.2 or higher.

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.

Note: For more information about configuring CA Workload Automation AE to work with Notification Services, see the *Windows Implementation Guide*.

CA Service Desk Support

CA Workload Automation AE supports CA Service Desk r11 through r12.5. CA Workload Automation AE lets you open a service desk ticket (request or incident) when a job fails.

Note: For more information about configuring CA Workload Automation AE to work with CA Service Desk, see the *UNIX Implementation Guide* or *Windows Implementation Guide*.

CA NSM Event Management Support

CA Workload Automation AE supports CA NSM Event Management r11.2 SP2. CA NSM Event Management lets you automate manual problem resolution tasks, filter and consolidate multiple events, monitor for unusual conditions, and take proper corrective action.

You can install the Event Agent on the CA Workload Automation AE server using the CA Common Components DVD.

Notes:

- For more information about installing the Event Agent, see the CA Common Components documentation.
- For more information about configuring CA Workload Automation AE to work with CA NSM Event Management, see the *UNIX Implementation Guide* or *Windows Implementation Guide*.

CAICCI Support

CA Workload Automation AE supports CAICCI (CA, Inc. Common Communications Interface) r11.2 SP2. CAICCI is the communication layer that lets the CA Workload Automation AE scheduler, which handles cross-platform events, to communicate with legacy agents on the distributed, midrange, and mainframe platforms.

You install CAICCI using the CA Common Components DVD.

Notes:

- For more information about installing CAICCI, see the CA Common Components documentation.
- For more information about configuring CA Workload Automation AE to work with CAICCI, see the *UNIX Implementation Guide* or *Windows Implementation Guide*.

CA NSM and CA UJMA Support

CA Workload Automation AE supports CA Network and Systems Management Job Management Option (CA NSM JMO) and CA Universal Job Management Agent (CA UJMA). CA UJMA lets CA Workload Automation AE schedule jobs to and receive job submissions from CA NSM JMO. CA Workload Automation AE can also submit jobs to CA NSM JMO. CA Workload Automation AE can also forward all workload-generated events to the CA NSM Event Management console.

Important! When you install CA Workload Automation AE components on a server that has any component of CA NSM r3.1 installed, you must follow these rules:

- If you do not want to perform cross-platform scheduling using CA Workload Automation AE, you can install CA Workload Automation AE on a server that has CA NSM r3.1 installed.

- After you install CA Workload Automation AE on a server, you can no longer install any CA NSM r3.1 components on that server. The CA NSM r3.1 components must be installed first.

- The CA Workload Automation AE scheduler (excluding the client and agent) only supports CA NSM r11.2 SP2 components, including the Job Management Option and Event Management. The r11.2 SP2 components are supported because CAICCI r11.x is required to perform cross-platform scheduling.

Note: For more information about configuring cross-platform scheduling, see the *UNIX Implementation Guide* or *Windows Implementation Guide*.

Chapter 8: Related Documentation

This chapter describes the documents provided with CA Workload Automation AE Release 11.3.6 and how to access them.

Important! The acknowledgements for third-party components used by CA Workload Automation AE are in the acknowledgements.txt file that is located in the root directory of the installed product.

This section contains the following topics:

CA Workload Automation AE Documentation

CA Workload Automation AE Release 11.3.6 includes the following documentation:

- CA Workload Automation AE Administration Guide

- CA Workload Automation AE Administrator Online Help

- CA Workload Automation AE Message Reference Guide

- CA Workload Automation AE Overview Guide

- CA Workload Automation AE Reference Guide

- CA Workload Automation AE Release Notes

- CA Workload Automation AE UNIX Implementation Guide

- CA Workload Automation AE User Guide

- CA Workload Automation AE Web Services Programming Guide

- CA Workload Automation AE Windows Implementation Guide

- CA Workload Automation Security Guide

- CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide

- CA Workload Automation Agent for UNIX, Linux, or Windows Release Notes

CA WCC Documentation

CA Workload Control Center (CA WCC) is the web-based user interface for CA Workload Automation AE. For more information about configuring and using CA WCC to manage your workload, see the documentation available on the CA WCC Release 11.3.6 DVD.

CA Common Components Documentation

CA Workload Automation AE and CA WCC integrate with CA Common Components including CA EEM, SSA, Event Management, Management Command Center, and CAICCI. You can install these common components using the CA Common Components Release 11.3.6 DVD.

The CA Common Components Release 11.3.6 DVD includes the following documentation:

- CA Common Components Implementation Guide

- CA Common Components Release Notes

- CA EEM Release Notes

- CA EEM Implementation Guide

- CA EEM Programming Guide

- CA NSM Inside Event Management and Alert Management Guide

Agent Documentation

The *Implementation Guides*, *Readmes*, and *Release Notes* for all the agents and agent plug-ins you can use to run various types of CA Workload Automation AE and third-party workload are available on CA Support (http://ca.com/support). On CA Support, select the CA Workload Automation System Agent bookshelf from the Find a Product Documentation Bookshelf section on the Documentation page.

Access the Documentation

To access the documentation in the product image, go to the Documentation directory of the appropriate image and open the Bookshelf.html file. The bookshelf links to the documentation set corresponding to that image.

To access all of the above documents from one location, with the ability to search across all of them, go to CA Support (http://ca.com/support) and select the CA Workload Automation AE bookshelf from the Find a Product Documentation Bookshelf section on the Documentation page.

Note: To view PDF files, you must download and install the Adobe Reader from the Adobe website if it is not already installed on your computer.

Release Numbers in Documentation

The release number on the title page of a document might not correspond to the current product release number; however, all documentation delivered with the product, regardless of release number on the title page, will support your use of the current product release. The release number changes only when a significant portion of a document changes to support a new or updated product release. If no substantive changes are made to a document, the release number does not change. For example, a document for r11 may still be valid for r11.3 or even r12. Documentation bookshelves always reflect the current product release number.

Occasionally, we must update documentation outside of a new or updated release. To indicate a minor change to the documentation that does not invalidate it for any releases that it supports, we update the edition number on the cover page. First editions do not have an edition number.