Contents

New Features in Release 11.3

This section contains the following topics:

New Product Name

In previous releases, the product name was Unicenter AutoSys Job Management.

Starting in r11.3, the product name is CA Workload Automation AE.

Note: AE represents AutoSys Edition.

New Agents

CA Workload Automation AE r11.3 supports new agents and agent plug-ins that let you automate, monitor, and manage workload on all major platforms, applications, and databases. To run workload on a particular system, you must install an agent on that system and add a machine definition to CA Workload Automation AE. You can install multiple agents on the same machine. Each agent on that machine must have a unique name and port number

The following agents are supported:

- CA Workload Automation Agent for i5/OS
- CA Workload Automation Agent for Linux
- CA Workload Automation Agent for UNIX
- CA Workload Automation Agent for Windows
- CA Workload Automation Agent for z/OS

Note: Starting in r11.3, CA Workload Automation Agent for UNIX, Linux, or Windows replaces the legacy remote agent that was available for r4.5 and r11. However, CA Workload Automation AE r11.3 provides backward compatibility with the legacy remote agent.

You can extend the functionality of the agent by installing one or more agent plug-ins into 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.

The following agent plug-ins are supported:

- CA Workload Automation Agent for Application Services
- CA Workload Automation Agent for Databases
- CA Workload Automation Agent for PeopleSoft
- CA Workload Automation Agent for Oracle E-Business Suite
- CA Workload Automation Agent for SAP
- CA Workload Automation Agent for Web Services

Notes:

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

For more information about configuring CA Workload Automation AE to work with agents, see the UNIX Implementation Guide or Windows Implementation Guide.

Location of the Agent Installation Files

The installers for the following agents are provided with CA Workload Automation AE r11.3:

- CA Workload Automation Agent for Linux
- CA Workload Automation Agent for UNIX
- CA Workload Automation Agent for Windows

Note: For more information about installing these agents, see the CA Workload Automation AE r11.3 UNIX Implementation Guide or Windows Implementation Guide.

The installation files for the following agents and agent plug-ins are located on the CA Workload Automation Agent r11.3 DVD:

- CA Workload Automation Agent for Application Services
- CA Workload Automation Agent for i5/OS
- CA Workload Automation Agent for Linux (zLinux)
- CA Workload Automation Agent for Databases
- CA Workload Automation Agent for PeopleSoft
- CA Workload Automation Agent for Oracle E-Business Suite
- CA Workload Automation Agent for SAP
- CA Workload Automation Agent for UNIX (Solaris-x86)
- CA Workload Automation Agent for Web Services

The installation file for CA Workload Automation Agent for z/OS is available on the CA Workload Automation EE media.

Note: For more information about installing these agents, see the Implementation Guide for the agent or agent plug-in that you want to install. The agent documentation is also located on the CA Workload Automation Agent r11.3 DVD.

Agent Local Security

CA Workload Automation Agent for UNIX, Linux, or Windows provides a local security feature that controls which users are allowed to submit jobs on behalf of other users.

The CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide describes how to specify these permissions using the following security rule:

x a | d manager_userID agent_userID path

However, the previous rule does not apply to CA Workload Automation AE.

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

The agent local security feature also supports the following rule, but this rule does not apply to CA Workload Automation AE:

c a | d manager_userID CONTROL command

This rule specifies which scheduling manager user IDs can issue control commands and send messages to an agent. Do not use this rule with CA Workload Automation AE.

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

New Job Types

The new agents and agent plug-ins let you define and run the following new job types:

Agent Name	Supported Job Types
CA Workload Automation Agent for UNIX or Linux	Command (CMD) CPU Monitoring (OMCPU) Disk Monitoring (OMD) File Trigger (FT) File Transfer Protocol (FTP) IP Monitoring (OMIP) Process Monitoring (OMP) Secure Copy (SCP) Text File Reading and Monitoring (OMTF)
CA Workload Automation Agent for Windows	Command (CMD) CPU Monitoring (OMCPU) Disk Monitoring (OMD) File Trigger (FT) File Transfer Protocol (FTP) IP Monitoring (OMIP) Process Monitoring (OMP) Secure Copy (SCP) Text File Reading and Monitoring (OMTF) Windows Event Log Monitoring Jobs (OMEL) Windows Service Monitoring (OMS)
CA Workload Automation Agent for Databases	Database Monitor (DBMON) Database Stored Procedure (DBPROC) Database Trigger (DBTRIG) Structured Query Language (SQL)
CA Workload Automation Agent for i5/OS	i5/OS (I5) All UNIX-based job types if they run in the PASE environment (see the job types listed for CA Workload Automation Agent for UNIX or Linux)
CA Workload Automation Agent for Oracle E-Business Suite	Oracle E-Business Suite Copy Single Request (OACOPY) Oracle E-Business Suite Request Set (OASET) Oracle E-Business Suite Single Request (OASG)
CA Workload Automation Agent for PeopleSoft	PeopleSoft (PS)
CA Workload Automation Agent for SAP	SAP Batch Input Session (SAPBDC) SAP BW InfoPackage (SAPBWIP) SAP BW Process Chain (SAPBWPC) SAP Data Archiving (SAPDA) SAP Event Monitor (SAPEVT) SAP Job Copy (SAPJC)

	SAP Process Monitor (SAPPM) SAP R/3 (SAP)
CA Workload Automation Agent for Application Services	Entity Bean (ENTYBEAN) Hypertext Transfer Protocol (HTTP) Java Remote Method Invocation (JAVARMI) JMS Publish (JMSPUB) JMS Subscribe (JMSSUB) JMX-MBean Attribute Get (JMXMAG) JMX-MBean Attribute Set (JMXMAS) JMX-MBean Create Instance (JMXMC) JMX-MBean Operation (JMXMOP) JMX-MBean Remove Instance (JMXMREM) JMX-MBean Subscribe (JMXSUB) Plain Old Java Object (POJO) Session Bean (SESSBEAN)
CA Workload Automation Agent for Web Services	Plain Old Java Object (POJO) Web Service (WBSVC)
CA Workload Automation Agent for z/OS	z/OS Data Set Trigger (ZOSDST) z/OS Manual (ZOSM) z/OS Regular (ZOS)

Notes:

The Command, Box, File Watcher, and User-defined job types are still supported in CA Workload Automation AE r11.3.

For more information about how these job types work, see the User Guide. For detailed information about the JIL syntax used to define these jobs, see the Reference Guide.

You can also use CA WCC to define jobs. For more information about using CA WCC to define the job, see the CA WCC documentation.

Job Types That Will Be Supported After r11.3

The following job types are referenced in the CA Workload Automation AE and agent guides but are not supported at the time of the r11.3 release:

- Micro Focus (MICROFOCUS)
- SNMP Value Get (SNMPGET)
- SNMP Value Set (SNMPSET)
- Wake on LAN (WOL)

These job types will be supported in a service pack or a later release of CA Workload Automation AE.

Support for Virtual Resources

You can now define virtual resources to CA Workload Automation AE and specify those resources as job dependencies. Virtual resources (depletable, renewable, and threshold) are representations that cannot be physically measured and are not directly tied to a physical system. You can manage shared resources to control concurrent access typically needed to enforce integrity and balance performance. For example, you can prevent jobs from running simultaneously and help ensure that a job is submitted only when the minimum number of resources is available.

If the scheduler is unable to run a job because virtual resources are not available, it will place the job in a new state: RESWAIT. The scheduler returns virtual resources when a job completes execution or when a job start failure occurs after a job acquires resources. You can send the new RELEASE_RESOURCE event to instruct the scheduler to return virtual resources held by a job. When an attempt to return resources fails, the RETURN_RESOURCE_FAIL alarm is issued. After virtual resources are returned, the scheduler evaluates jobs that are in the RESWAIT state and submits qualifying jobs for execution.

For more information about how resources and resource job dependencies work, see the User Guide. For detailed information about the JIL syntax used to define resources and resource job dependencies or about the sendevent command used to send the RELEASE_RESOURCE event, see the Reference Guide.

New Machine Type

By default, all new machine definitions are set to type-a. Type-a machines represent the new agent and require new machine attributes representing the agent name, type of data encryption, encryption key, and so on. To use operating system-specific features of CA Workload Automation AE, type-a machines also require the setting of the opsys attribute. The opsys attribute represents the operating system of the computer where the agent is installed.

For more information about the opsys attribute and other machine attributes, see the Reference Guide.

Cross-Instance Job Dependencies with CA Workload Automation EE

You can define and monitor cross-instance (external) job dependencies between CA Workload Automation AE and CA Workload Automation EE. These job dependencies let you create job flows between distributed and mainframe systems.

For more information about how external job dependencies work, see the User Guide.

For detailed information about the commands and JIL syntax used to define external job dependencies, see the Reference Guide.

Must Start Times and Must Complete Times

You can use the new must_start_times job attribute to define the time or a list of times that a job must start by. The must_start_times attribute generates the CHK_START event to instruct the scheduler to check whether a job has started by the specified time.

If the job does not start by the specified time, the MUST_START_ALARM alarm is issued.

Similarly, you can use the new must_complete_times attribute to define the time or a list of times that a job must complete by. The must_complete_times attribute generates the CHK_COMPLETE event to instruct the scheduler to check whether a job has completed by the specified time. If the job does not complete by the specified time, the MUST_COMPLETE_ALARM alarm is issued.

Defining must start times and must complete times is helpful when you want to be notified when a job has not started or completed on time.

For more information about the must_start_times and must_complete_times attributes, see the Reference Guide.

Manual Intervention for i5/OS Job Types and the New REPLY_RESPONSE Event

You can define an i5/OS job to schedule workload to run on an i5/OS system. The job can run a program or an i5/OS command. You can run i5/OS jobs in the root file system, open systems file system (QOpenSys), and library file system (QSYS).

A program run on an i5/OS system may require additional feedback from the end user before it can continue execution. The CA WA Agent for i5/OS notifies the scheduler when a manual response is required. In this case, the scheduler raises a WAIT_REPLY_ALARM and places the job in a new state: WAIT_REPLY. The text of the WAIT_REPLY_ALARM contains the query of the i5/OS program and may show the expected responses. You must send a REPLY_RESPONSE event with a valid response in order for the job to proceed. When the scheduler experiences a problem communicating with the CA WA Agent for i5/OS to send the REPLY_RESPONSE event, the REPLY_RESPONSE_FAIL alarm is raised. The CA WA Agent for i5/OS resumes sending job status updates to the scheduler upon receipt of an accepted response.

For more information about i5/OS jobs, see the User Guide. For detailed information about the REPLY_RESPONSE event, see the Reference Guide.

New as_test Command

The as_test command is a utility that can run for a specified amount of time, write a message to stdout and/or stderr, and exit with a specific exit code. When the scheduler is running in test mode to agents, Command job commands are automatically replaced with the execution of this command. You can use as_test to test job dependencies and error handling.

For more information about the as_test command, see the Reference Guide. For information about test mode, see the Administration Guide.

New forecast Command

You can report future job flows by using the new forecast command. The reported job flow displays a list of future jobs based on the dates you specify. Forecast reports can help you predict what occurs when a set of conditions is predefined. You can see what happens when values are changed for each forecast period and use this information to plan your workflow.

For more information about the forecast command, see the Reference Guide.

New archive_jobs Command

You can remove obsolete job versions from the database by using the new archive_jobs command. The archive_jobs command can help prevent the database from being overloaded with obsolete job versions. We recommend that you issue the archive_events command before issuing the archive_jobs command.

For more information about the archive_jobs command, see the Reference Guide.

New autoprofm Command

Valid on Windows only

To upgrade to CA Workload Automation AE r11.3, your profiles must be converted to a file format that works with the new CA Workload Automation Agent. The profiles are automatically converted during the upgrade process. However, you can also manually convert profiles by using the new autoprofm utility.

For more information about the autoprofm utility, see the Reference Guide.

New Scheduler Startup Settings on UNIX

You can configure the following startup settings for the scheduler on UNIX:

Global Auto Hold mode

You can specify whether to start the scheduler in Global Auto Hold mode. Starting the scheduler in Global Auto Hold mode prevents the system from being flooded with jobs that were scheduled to run during a down time. When the scheduler starts after a down time, it puts all jobs that are eligible to run in an ON_HOLD status. You can then selectively start jobs by sending a FORCE_STARTJOB event.

Chase on Startup mode

You can specify whether the chase command runs when the scheduler starts. The chase command verifies whether jobs and agents are running. You can track network problems if you run the chase command at regular intervals.

For more information about configuring these settings on UNIX, see the Administration Guide.

These settings were already supported on Windows. For more information about configuring these settings on Windows, see the Online Help for CA Workload Automation AE Administrator (autosysadmin)

Monitoring a Condition Continuously and the New ALERT Event

You can define the following job types to monitor a condition continuously:

- CPU Monitoring (OMCPU)
- Database Monitor (DBMON)
- Database Trigger (DBTRIG)
- Disk Monitoring (OMD)
- File Trigger (FT)
- Text File Reading and Monitoring (OMTF)
- Windows Event Log Monitoring (OMEL)
- Windows Services Monitoring (OMS)

Each time the specified condition occurs, an ALERT event is written to the scheduler log file (event_demon.$AUTOSERV on UNIX and event_demon.%AUTOSERV% on Windows).

These events are also displayed when you create a report using the autorep -J -d command. The report includes the events that are generated during the most recent job runs.

To stop a continuous monitor, you must complete the job manually by issuing the sendevent –E KILLJOB command.

For more information about how these job types monitor conditions continuously, see the User Guide. For detailed information about the JIL syntax used to monitor a condition continuously, see the Reference Guide.

Logging a Job's State Changes and the New STATE_CHANGE Event

Some of the new job types go through different state changes when they run. For example, a z/OS Regular job can go through state changes for each step that runs. The scheduler log file (event_demon.$AUTOSERV on UNIX and event_demon.%AUTOSERV% on Windows) records the job's state changes using the new STATE_CHANGE event.

These events are also displayed when you create a report using the autorep -J -d command. The report includes the events that are generated during the most recent job runs

Improved Log Maintenance

You can specify when the scheduler or the application server log rolls over. When the log rolls over, the data is saved in a backup file with a date and time stamp. The log can roll over at a specified time or when the log file size is equal to a specified size.

On UNIX, you can configure this setting using the new LOGROLLOVER parameter in the configuration file. For more information about this parameter, see the Administration Guide.

On Windows, you can configure this setting by modifying the LOGROLLOVER environment variable in the System window of CA Workload Automation AE Administrator (autosysadmin). For more information about this setting, see the Online Help for CA Workload Automation AE Administrator.

Specifying the localhost

In r11.3, the localhost machine name is a reserved name. You can no longer define a machine for localhost by creating an insert_machine: localhost definition. By default, the localhost value is resolved to the name of the machine where the CA Workload Automation AE scheduler was started. You can override the reserved localhost value to the name of another real machine by using the new local machine definition setting.

On UNIX, you can configure this setting using the LocalMachineDefinition parameter in the configuration file. For more information about this parameter, see the Administration Guide.

On Windows, you can configure this setting using the Local Machine Definition field in the Scheduler window of CA Workload Automation AE Administrator (autosysadmin).

For more information about this field, see the Online Help for CA Workload Automation AE Administrator.

For more information about how the localhost value is resolved when a job runs, see the User Guide.

Appending Event Message Text in Scheduler Log File

You can append the text associated with an event to the corresponding event message in the scheduler log file. Appending the text can help when you want to write event policies with Event Management. Alternatively, you can print the text as a standalone message in the scheduler log file.

On UNIX, you can configure this setting using the new AppendEventMessageText parameter in the configuration file. For more information about this parameter, see the Administration Guide.

On Windows, you can configure this setting using the new Append Event Message Text field in the Scheduler window of CA Workload Automation AE Administrator (autosysadmin). For more information about this field, see the Online Help for CA Workload Automation AE Administrator.

Specifying an Instance-Wide Encryption Key

You can specify the instance-wide encryption key for all communication between the CA Workload Automation AE components of the same instance.

On UNIX, you can configure this setting using the new UseEncryption parameter in the configuration file. For more information about this parameter, see the Administration Guide.

On Windows, you can configure this setting using the new Use Instance Wide AES 128-bit Data Encryption check box in the Instance window of CA Workload Automation AE Administrator (autosysadmin). For more information about this setting, see the Online Help for CA Workload Automation AE Administrator.

Polling for Resource Availability

You can specify how frequently the scheduler polls for resource availability when jobs are waiting on resources.

On UNIX, you can configure this setting using the new ResourceWaitPollInterval parameter in the configuration file. For more information about this parameter, see the Administration Guide.

On Windows, you can configure this setting using the new Res Wait Poll Interval field in the Instance window of CA Workload Automation AE Administrator (autosysadmin). For more information about this field, see the Online Help for CA Workload Automation AE Administrator.

New reindex.pl Script for Rebuilding Database Table Indexes

The new reindex.pl script rebuilds the table indexes of a specified CA Workload Automation AE database. This script is located in the $AUTOSYS/dbobj directory (UNIX) or %AUTOSYS%\dbobj directory (Windows).

For more information about the reindex.pl script, see the Administration Guide.

Changes in Release 11.3

This section contains the following topics:

Legacy Agent Replaced by CA Workload Automation Agent

The new CA Workload Automation Agent for UNIX, Linux, or Windows replaces the Remote Agent (auto_remote) that was provided with Unicenter AutoSys JM r4.5 and r11. The r11.3 documentation refers to auto_remote as the legacy agent.

The new agent provides additional job types, including monitoring and FTP jobs. The agent is automatically installed on the computer where CA Workload Automation AE is installed. You can also install the agent on remote computers to run jobs on those computers.

Differences between the Legacy Agent and the New Agent

In addition to the new job types supported by the new agents and agent plug-ins, other agent features and behaviors were changed for this release. This section describes the differences between the legacy agent and the new agent.

Note: The CA Workload Automation AE Administrator utility is the name of the autosysadmin

Location of Log Files

In r4.5 and r11, the legacy agent's log files were written to the following locations:

- UNIX—The directory specified in the AutoRemoteDir parameter in the $AUTOUSER/config.$AUTOSERV configuration file
- Windows—The directory specified in the Enterprise Wide Logging Directory field in the Administrator utility

Note: In r11.3, the name of this field was changed to Legacy Enterprise Wide Logging Directory.

In r11.3, those logging directories are only used when running jobs on the legacy agents.

The new agent in r11.3 writes all log files to the following directories:

- installation_directory/SystemAgent/agent_name/log
- installation_directory/SystemAgent/agent_name/spool (for job spool files)

Note: In r4.5 and r11, you had to override the default log file directory on operating systems that do not support the locking of files in the /tmp directory. This is because the agent used the locks to check whether a job was running. You no longer have to change the default log file directory because the new agent stores the job spool files in the installation_directory/SystemAgent/agent_name/spool directory by default. However, you must change the default log file directory if you run jobs on legacy agents and the operating system on any of the legacy agent computers does not support the locking of files in the /tmp directory.

CA Workload Automation AE Configuration on the Agent

To communicate with the new agent, your CA Workload Automation AE instance must be specified in the agent's agentparm.txt configuration file. Certain parameters defined on CA Workload Automation AE and the agent must match.

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

Communication Port

The configuration required to communicate with the new agent is different from the configuration for the legacy agent.

In r4.5 and r11, the scheduler used the following port setting to communicate with the legacy agent:

- UNIX—The AutoRemPort parameter in the $AUTOUSER/config.$AUTOSERV configuration file
- Windows—The Remote Agent Port field in the Administrator utility

Note: In r11.3, the name of this field was changed to Legacy Remote Agent Port.

In r11.3, you can use those port values to communicate with the legacy agent. Those port values do not apply to the new agent.

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

Environment Variables

In r4.5 and r11, the legacy agent's environment was set by sourcing the environment variables specified in the /etc/auto.profile file. The variables are preceded by #AUTOENV#.

- In r11.3, the environment variables are specified in the following locations:
- Agent-wide environment variables in the agent's agentparm.txt file
- Manager-specific environment variables in the agent's agentparm.txt file
- The profile JIL attribute in a job definition
- The envvars JIL attribute in a job definition

Note: For more information about the parameters in the agentparm.txt file, see the CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide. For more information about setting profiles and environment variables in a job definition, see the User Guide.

Log File Maintenance

In r4.5 and r11, the following settings specified whether the legacy agent's temporary log files were automatically removed:

- UNIX—The CleanTmpFiles parameter in the $AUTOUSER/config.$AUTOSERV configuration file
- Windows—The Clean Temporary Files field in the Administrator utility

Note: In r11.3, the name of this field was changed to Legacy Clean Temp Files.

In r11.3, those settings are only used for legacy agent log files.

The new agent has parameters in the agentparm.txt file that control how log files and job spool files are maintained.

Note: For more information about maintaining agent log files and clearing job spool files, see the CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.

Minimum Disk Space Used for Logging

In r4.5 and r11, the following settings specified the minimum amount of disk space that must be available to write to the scheduler log:

- UNIX—The FileSystemThreshold parameter in the $AUTOUSER/config.$AUTOSERV configuration file
- Windows—The FileSystem Threshold KB field in the Administrator utility

In r11.3, those settings are only used when running jobs on the legacy agents.

The new agent has parameters in the agentparm.txt file that control the log file settings.

Note: For more information about the log file settings, see the CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.

Remote Profile Files

In r4.5 and r11, the following settings specified whether the scheduler redirects all standard error and standard output information to the auto.rem* log file:

- UNIX—The RemoteProFiles parameter in the $AUTOUSER/config.$AUTOSERV configuration file
- Windows—The Remote Profile Logging check box in the Administrator utility

Note: In r11.3, the name of this field was changed to Legacy Remote Profile Logging.

The output information is generated when the /etc/auto.profile file is sourced.

In r11.3, those settings are only used when running jobs on the legacy agents.

The new agent does not use these settings or writes any output generated by the /etc/auto.profile file.

Note: For more information about the remote profile files settings, see the Administration Guide (UNIX) or the Online Help for the Administrator utility (Windows).

Debugging Logs

In r4.5 and r11, the ISDBGACTIV setting controlled the display of trace messages for debugging.

In r11.3, the administrator for the new agent can set the log.level parameter in the agent's agentparm.txt file. This parameter controls the type of debugging logs that are generated.

Note: For more information about log.level parameter, see the CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.

Signals for a KILLJOB Event

In r4.5 and r11, you can specify a comma-separated list of signals to send to a job whenever the KILLJOB event is sent. The following settings specified the signals:

- UNIX—The KillSignals parameter in the $AUTOUSER/config.$AUTOSERV configuration file
- Windows—The Kill Signals field in the Administrator utility

Note: In r11.3, the name of this field was changed to Legacy Kill Signals.

In r11.3, those settings are only used when running jobs on the legacy agents.

Calculating Machine Load

In r4.5 and r11, you can define the method used to determine the percentage of CPU cycles available on a real machine that belongs to a virtual machine. The following settings specified the method:

- UNIX—The MachineMethod parameter in the $AUTOUSER/config.$AUTOSERV configuration file
- Windows—The Machine Method field in the Administrator utility

In r11.3, the agent does not use the UNIX vmstat utility or Windows performance counters to determine the percentage of available CPU. Instead, the new agent runs a CPU Monitor job to determine the current load on the machine.

The rstatd method continues to be supported by the UNIX scheduler. However, for this method to be used, the value of the opsys attribute for a type-a machine definition must be set to an operating system that supports rstatd ('aix', 'hpux', ' linux', 'openvms', or 'solaris.'). If the value of the opsys attribute is not set or is set to an operating system that does not support rstatd, the UNIX scheduler will use a CPU Monitor job to calculate the available machine load.

Running Windows Commands

You can define Command jobs to run Windows operating system commands, such as dir and echo. In r4.5 and r11, you specified only the command and arguments in the command attribute (for example, command: "dir c:\temp\"). The legacy agent prefixed "path\cmd.exe /c" to the command before running the process.

In r11.3, the new agent does not automatically prefix the command with the path to the command interpreter. To automatically prefix the command, you must set the followingparameters in the agent's agentparm.txt file to true:

oscomponent.lookupcommand=true

oscomponent.cmdprefix.force=true

If these agent parameters are not set, you must explicitly invoke the command interpreter in the command attribute, as shown in the following example:

command: "c:\winnt\system32\cmd.exe /c dir c:\temp\"

Note: For more information about the command attribute, see the Reference Guide and User Guide. For more information about the agent parameters, see the CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.

Polling Interval for File Watcher Jobs

In r11.3, you can define a File Watcher (FW) job to run on a machine that has the legacy agent or the new agent installed. The behavior of the new agent for the polling interval is different from the legacy agent.

The legacy agent uses a default polling interval of 60 seconds for a FW job. You can override this value by specifying the watch_interval attribute in a job definition.

The r11.3 agent uses two polling intervals for a FW job: a global default of 30 seconds set on the agent and the watch_interval attribute value specified in the job definition. If the condition the FW job is monitoring is not satisfied, the agent sleeps for 30 seconds based on its global polling interval. After 30 seconds, the agent checks the condition of the file again. If the condition is satisfied, the agent waits for the second polling interval specified by the watch_interval attribute to ensure the file remains steady. If the file has not changed after the second polling interval elapses, the agent returns the status. If the file does change, the agent goes back to sleep for the duration of the second polling interval until the file eventually stabilizes.

Evaluation of Job's Termination Time

If a job runs on a machine that has the new agent installed, the scheduler evaluates the term_run_time attribute and automatically generates a CHK_TERM_RUNTIME event to instruct the scheduler to check whether a job has ended by the specified time. If the job does not end by the specified time, the scheduler sends the agent a request to kill the job. If a job runs on a machine that has the legacy agent installed, the legacy agent evaluates the term_run_time attribute and no CHK_TERM_RUNTIME event is generated. If the job does not end by the specified time, the legacy agent terminates the job. If the job does not end by the specified time, the legacy agent terminates the job.

Job Attribute Environment Variables

The new CA Workload Automation Agent no longer supports the setting of job definition JIL attributes as environment variables. Custom job applications that require knowledge of the job's attributes should be rewritten to invoke the GetJobsWithFilter class of the C++ or Java SDK.

Encryption and FIPS 140-2 Compliance

In r11, CA Workload Automation AE used SSL encryption. In the current release, CA Workload Automation AE uses Advanced Encryption Standard (AES) encryption to comply with the U.S. Government encryption standard FIPS 140-2. This standard requires a FIPS-certified library and FIPS-certified cipher algorithm, such as AES.

CA Workload Automation AE uses the AES cipher algorithm to encrypt and decrypt data shared between the command line utilities, agent, scheduler, and the application server.

Encryption requires eTrust Public Key Infrastructure (ETPKI), which is automatically installed with the server, agent, or client.

AES also requires an encryption key. You can modify the key for the following components:

- Application server and client utilities—The key is stored in the $AUTOUSER/cryptkey.txt file.
- Application server and agent—The key is specified in the machine definition for the agent. This key must match the key in the agent's cryptkey.txt file. The cryptkey.txt file is located in the installation_directory/SystemAgent/agent_name directory.
- Scheduler and agent—The key is specified in the machine definition for the agent.

  This key must match the key in the agent's cryptkey.txt file. The cryptkey.txt file is located in the installation_directory/SystemAgent/agent_name directory.

Note: For r11.3, CA Workload Automation AE supports AES encryption only. While the product still supports running SSL encryption over SSA, the preferred data encryption method is AES (SSL encryption under SSA is disabled by default when SSA is installed).

For more information about configuring encryption, see the Security Guide.

Pound Sign (#) Allowed in Object Names

The pound sign or hash character (#) is now allowed in all object names (for example, job and calendar names).

Command Substitutions Not Allowed in the watch_file Attribute

In 4.0 and r4.5, you could use back ticks or the grave accent (`) to specify command substitutions in the watch_file attribute.

In r11 and r11.3, you cannot use back ticks when you specify the path in the watch_file attribute. For example, the watch_file attribute cannot resolve the date if you specify the path as follows:

watch_file: \tmp\`date`

Removed Commands

The following commands have been removed from CA Workload Automation AE r11.3:

- autodwp
- autosys_report—This application is now part of CA Workload Automation AE Administrator (Windows only).
- autosys_wv
- job_delete—This command has been replaced by the archive_jobs command.
- job_profiles—This application is now part of CA Workload Automation AE Administrator (Windows only).
- ntgetdate
- xql
- zql

Scheduler Startup Options Removed from the eventor Command

In the previous release, the eventor command let you specify whether the scheduler starts in Global AutoHold mode (eventor -G option) and whether to run the chase command at startup (eventor -n option). These two options have been removed from the eventor command.

Instead, you can now control the startup behavior of the scheduler by using the new GlobalAutoHold and ChaseOnStartup options in the configuration file (config.$AUTOSERV file).

Note: For more information about configuring these startup settings on UNIX, see the Administration Guide. For more information about configuring these startup settings on Windows, see the Online Help for CA Workload Automation AE Administrator (autosysadmin).

Job Profiles Manager and autosysreport.exe Integrated with the Administrator Utility

Valid on Windows

The following tools are now part of the Administrator utility:

- Job Profiles Manager
- Feedback or Report Tool (autosysreport.exe)

Changes to Cross-Instance Job Dependencies

Cross-instance job dependencies have changed as follows:

- To improve efficiency, external events are now stored in a new database table named ujo_ext_event.
- To define cross-instance job dependencies between r11.3 and 4.5, a new lightweight application server that supports 4.5 is installed on the r11.3 instance.
- You can now define cross-instance job dependencies between CA Workload Automation AE instances that have different encryption settings. You specify the external instance's encryption key using the xcrypt_key attribute when you define the instance to CA Workload Automation AE.

Note: For more information about configuring your instance, see the UNIX Implementation Guide or Windows Implementation Guide. For more information about defining cross-instance job dependencies, see the User Guide.

Updated autoping Command

The -S option has been added to the autoping command to test the connectivity between the application server and the new CA Workload Automation Agent.

Note: If you issue autoping -M [machine] -S against the legacy agent, the command reverts to its previous behavior and tests the database connectivity between CA Workload Automation AE and the agent.

Updated clean_files Command

The clean_files command now applies to legacy agent log files only. For more information about maintaining the log files and spool files for the new agent, see the CA Workload Automation Agent for UNIX, Linux, or Windows Implementation Guide.

IPv6 Support

CA Workload Automation AE r11.3 supports Internet Protocol version 6 (IPv6) between CA Workload Automation AE r11.3, CA 7, CA Workload Automation EE, and agents.

The Job Information Language (JIL) utility now accepts IPv6 addresses in addition to hostnames and IPv4 addresses. For example, when you use the jil command to define a new machine, you can specify an IPv6 address in the machine attribute.

Change in as_owner Policy Validation

In R11.3, CA Workload Automation AE validates the as_owner policy using either the owner specified by the owner attribute in the job definition or the default owner of the job.

KILLJOB and SEND_SIGNAL Behavior

The following new alarms are generated when the scheduler experiences a problem communicating with the agent while killing a job or sending a signal:

- KILLJOBFAIL – generated when the attempt to kill a job fails
- SENDSIGFAIL– generated when the attempt to send a signal fails

Although Windows agents do not support sending signals to jobs, you can signal a named Windows semaphore. To signal a named Windows semaphore, set the value of the opsys attribute for a type-a machine to the Windows operating system (‘windows’).

New Features in Release 11.3 SP1

No new features were added in CA Workload Automation AE Release 11.3 SP1.

Changes in Release 11.3 SP1

This section contains the following topics:

Alarm Removed

The APP_SERVER_COMM alarm is removed from CA Workload Automation AE.

Creating a Forecast Report for Multiple Days

In the current release, you can specify any time frame when creating a forecast report. You can specify the time frame for a forecast report using the -F and -T attributes of the forecast command. In the previous release, you could specify a time frame up to 24 hours. There are now no limits on the number of days you can specify; however, reports with longer time frames consume more memory and time.

New Features in Release 11.3.5

This section contains the following topics:

New Job Types

The agent and agent plug-ins let you define and run the following new job types:

Agent or Agent Plug-in Name	Supported Job Types
CA Workload Automation Agent for UNIX, Linux, or Windows	Simple Network Management Protocol Value Get (SNMPGET) Simple Network Management Protocol Value Set (SNMPSET) Wake on LAN (WOL)
CA Workload Automation Agent for Micro Focus	Micro Focus (MICROFOCUS) This job type is supported only on the Windows environment.
CA Workload Automation Agent for Remote Execution	Remote Execution (PROXY)
CA Workload Automation Agent for Web Services	Web Service Document/Literal (WSDOC) Process Automation Process Execution (PAPROC) Process Automation Start Request Form (PAREQ)

Notes:

- For more information about how these job types work, see the User Guide. For detailed information about the JIL syntax used to define these jobs, see the Reference Guide.
- You can also use CA WCC to define jobs. For more information about using CA WCC to define the job, see the CA WCC documentation.

New Web Server Component

In the current release, CA Workload Automation AE uses Apache Tomcat, which is the designated web server that is used to host web services. This web server is installed and configured as part of the CA Workload Automation AE installation. Apache Tomcat uses the CA Workload Automation AE configuration parameters for database access and security.

Note: For more information about the web server, see the UNIX Implementation Guide or the Windows Implementation Guide.

New Security Classes and Policies

The following new resource class and policies are added in this release:

- The as-base-jobtype resource class and its default policy with EXECUTE access mode is added to support the authorization of jobs based on their job types.
- The AGGREGATE policy is added in the as-control resource class. The AGGREGATE policy controls whether you can aggregate CA Workload Automation AE statistics.

New CA EEM Global User Group for CA Workload Automation AE

The current release introduces a new pre-defined CA EEM global user group named WorkloadAutomationAEWebService. The WorkloadAutomationAEWebService user group is empty by default, but you can add CA EEM users to it. Only members of the WorkloadAutomationAEWebService user group are authorized to access the CA Workload Automation AE web service.

Note: For more information about WorkloadAutomationAEWebService user group, see the CA Workload Automation Security Guide.

The Compliance Application

The compliance application is used to audit the system utilization. It installs automatically with CA Workload Automation AE and runs as part of the DBMaint command.

Note: For more information about the compliance application, see the UNIX Implementation Guide or the Windows Implementation Guide.

The Configuration File on Windows

In the previous releases, the configuration file was used to set the configuration parameters only on UNIX. On Windows, the CA Workload Automation AE Administrator was used to set the configuration parameters and these configuration parameters were stored in the Windows Registry.

In the current release, you can set the configuration parameters on Windows by using the CA Workload Automation AE Administrator or the configuration file. However, we recommend that you use the CA Workload Automation AE Administrator to set the configuration parameters on Windows. The configuration parameters that you set using the CA Workload Automation AE Administrator are stored in the configuration file.

Note: For information about the configuration file and the configuration parameters, see the Administration Guide. For information about configuring CA Workload Automation AE using the CA Workload Automation AE Administrator, see the Online Help.

Oracle Database Creation

In Unicenter AutoSys JM r11 and CA Workload Automation AE r11.3, you specified the Oracle administrator user and password during the installation. The installer used this information to create the Oracle database tablespaces, users, and roles.

In the current release, before you install CA Workload Automation AE, you can run the waae_oracle.sql script to create the Oracle database tablespaces, users, and roles. The installer does not prompt you to specify the Oracle administrator user and password information.

Note: For more information about the waae_oracle.sql script, see the UNIX Implementation Guide or the Windows Implementation Guide.

Repair an Existing Installation on UNIX

In the current release, the installer does the following when you repair an existing installation:

- Uses the RefreshAEDB script to repair the CA Workload Automation AE database.
- Regenerates the agentparm.txt file and the instance profile files.

Note: For more information about the RefreshAEDB script and about repairing an existing installation, see the UNIX Implementation Guide.

SNMP Support on Windows

You can configure CA Workload Automation AE to send SNMP traps to SNMP managers.

In the previous releases, this feature was supported only on UNIX. In the current release, it is supported on both UNIX and Windows.

Note: For more information about configuring CA Workload Automation AE to send SNMP traps, see the Administration Guide or the Online Help.

Support for CA Workload Automation Agent for Oracle E-Business Suite r11.3.1

CA Workload Automation Agent for Oracle E-Business Suite r11.3.1 includes the following new features:

- Quote resolved expressions in default values
- Give a higher priority to request set defaults over concurrent program defaults
- Specify value set expressions to resolve profile and flexfield expressions in SQL statements
- Specify the output format, template language, and template territory settings for the layout template
- Specify a list of Oracle users to notify when the job completes
- Identify request sets, single request programs, and Oracle users by display name or short name

Global Variable Substitution

Support for global variable substitution has been added to several CA Workload Automation AE attributes. You can reference a global variable as part of the syntax of any of the following attributes:

- command
- connect_string
- destination_file
- ftp_local_name
- ftp_remote_name
- i5_library_list
- i5_name
- i5_params
- monitor_cond
- scp_local_name
- scp_remote_dir
- scp_remote_name
- sp_name
- sql_command
- std_err_file
- std_in_file
- std_out_file
- success_criteria
- tablename
- text_file_name
- trigger_cond
- watch_file

Note: For information about global variables, see the User Guide. For more information about these attributes, see the Reference Guide.

Controlling the Starting of Jobs in PEND_MACH Status

You can control the starting of jobs in PEND_MACH status in the following ways:

- By defining the time interval (in seconds) that the scheduler waits before starting jobs in PEND_MACH status when an offline machine returns to service.
- By defining the burst value. The burst value defines the number of jobs in PEND_MACH status that the scheduler starts after waiting for the specified interval.

On UNIX, you can configure this setting using the GlobalPendMachInterval parameter in the configuration file. For more information about this parameter, see the Administration Guide.

On Windows, you can configure this setting using the Global Pend Mach Interval field on the Scheduler window of CA Workload Automation AE Administrator (autosysadmin).

For more information about this field, see the Online Help for CA Workload Automation AE Administrator.

Controlling the Status of Jobs Scheduled on an Offline Machine

You can control the status of jobs that are scheduled on a machine that is currently offline in the following ways:

- By defining the completion status that the scheduler assigns to jobs that are scheduled on an offline machine. On UNIX, you can configure this setting using the GlobalPendMachStatus parameter in the configuration file. On Windows, you can configure this setting using the Global Pend Mach Status field on the Scheduler window of CA Workload Automation AE Administrator (autosysadmin). The jobs temporarily remain in PEND_MACH status before the scheduler assigns the status specified in the GlobalPendMachStatus parameter (on UNIX) or the Global Pend Mach Status field (on Windows).
- By defining the time interval (in seconds) that the scheduler waits before updating the status of the job to the status specified in the GlobalPendMachStatus parameter (on UNIX) or the Global Pend Mach Status field (on Windows). On UNIX, you can configure this setting using the GlobalPendMachDelay parameter in the configuration file. On Windows, you can configure this setting using the Global Pend Mach Delay field on the Scheduler window of CA Workload Automation AE Administrator (autosysadmin).

Skipping Starting Condition Evaluation for Queued Jobs

In the current release, CA Workload Automation AE automatically re-evaluates the starting conditions for queued jobs when those jobs leave the queue. The jobs only start if conditions permit.

You can configure CA Workload Automation AE to skip evaluation of starting conditions for queued jobs, so the jobs start as soon as they leave the queue regardless of starting conditions.

On UNIX, you can configure CA Workload Automation AE to skip starting condition evaluation for queued jobs using the EvaluateQueuedJobStarts parameter in the configuration file. For more information about skipping starting condition evaluation for queued jobs on UNIX, see the Administration Guide.

On Windows, you can configure CA Workload Automation AE to skip starting condition evaluation for queued jobs using the Evaluate Queued Job Starts check box on the Scheduler window of CA Workload Automation AE Administrator (autosysadmin). For more information about skipping starting condition evaluation for queued jobs on Windows, see the Online Help.

Bypassing a Job to Run Downstream Dependent Jobs

You can now bypass a job to run downstream dependent jobs. To bypass a job use the sendevent -E JOB_ON_NOEXEC command. This command sets the job status to ON_NOEXEC and instructs the scheduler to bypass the execution of the job. CA Workload Automation AE evaluates ON_NOEXEC jobs as successfully completed even though CA Workload Automation AE does not execute the commands for these jobs.

CA Workload Automation AE reports the machine field for jobs in ON_NOEXEC status as "**NOEXEC**" to reflect that these jobs were not executed on any computer.

Downstream dependent jobs still run and boxes with ON_NOEXEC jobs evaluate as if the ON_NOEXEC jobs or boxes had run to success.CA Workload Automation AE continues to bypass jobs in ON_NOEXEC status until it receives and processes the JOB_OFF_NOEXEC event.

Sending Email Notifications

You can configure CA Workload Automation AE to send email notifications to operators or administrators who resolve problems or attend to emergencies.

On UNIX, you can configure this setting using the NotifyMethod, NotifySMTPHost, UseSMTPAuthentication, NotifySMTPUser, and NotifySMTPFromAddress parameters in the configuration file. For more information about these parameters, see the Administration Guide.

On Windows, you can configure this setting using the Method, SMTP Host, SMTP Server Requires Authentication, SMTP User, SMTP Password, and SMTP From Address fields on the Integration window of CA Workload Automation AE Administrator (autosysadmin). For more information about these fields, see the Online Help for CA Workload Automation AE Administrator.

Note: You must specify the send_notification, notification_emailaddress, and the notification_msg attributes in your job definition to send an email notification using CA Workload Automation AE. The notification_emailaddress is a new attribute that lets you specify multiple email addresses of the users to receive the email notification. For more information about these attributes, see the Reference Guide.

Aggregate Statistics

In Unicenter AutoSys JM r11 and CA Workload Automation AE r11.3, the autoaggr command was used to aggregate statistics into the hourly, daily, weekly, and monthly tables. In the current release, the autoaggr command generates reports based on the aggregated job, alarm, and scheduler statistics retrieved from the database.

You can now aggregate the job, alarm, and scheduler statistics into the database tables in the following ways:

- Manually by using the sendevent command. For more information about the sendevent command, see the Reference Guide.
- Automatically by configuring the AggregateStatistics parameter (on UNIX) or Aggregate Statistics field (on Windows). For more information about these configuration options, see the Administration Guide or the Online Help for CA Workload Automation AE Administrator.

Allowing the Shadow Scheduler to Failback to the Primary Scheduler

You can now configure CA Workload Automation AE to allow the shadow scheduler to failback to the primary scheduler. In a failed-over state, the primary scheduler shuts down and the shadow scheduler takes over processing events. To allow the primary scheduler to resume processing events when the shadow scheduler fails or when you shut it down, specify a primary failback mode that allows failbacks.

On UNIX, you can configure the primary failback mode using the PrimaryFailbackMode parameter in the configuration file. For more information about this parameter, see the Administration Guide.

On Windows, you can configure the primary failback mode using the Primary Failback Mode options on the Scheduler window of CA Workload Automation AE Administrator (autosysadmin). For more information about this field, see the Online Help for CA Workload Automation AE Administrator.

Enabling FIPS Mode

The Federal Information Processing Standards (FIPS) publications set guidelines for best practices for software and hardware computer security products. In FIPS mode, CA Workload Automation AE complies with the standards in FIPS 140-2: Security Requirements for Cryptographic Modules. CA Workload Automation AE supports FIPS 140-2: Security Requirements for Cryptographic Modules. You can configure CA Workload Automation AE to operate in FIPS mode, so it only uses security algorithms that comply with the guidelines in the FIPS 140-2 publication.

On UNIX, you can enable FIPS mode using the EnableFIPSMode parameter in the configuration file. For more information about this parameter, see the Security Guide.

On Windows, you can enable FIPS mode using the Enable FIPS Mode check box on the Instance window of CA Workload Automation AE Administrator (autosysadmin). For more information about enabling FIPS mode on Windows, see the Online Help.

Disabling IP Address Caching

By default, CA Workload Automation AE caches the IP addresses of the computers that it connects to for running jobs or any other communication. CA Workload Automation AE automatically recovers from a dynamic IP address when the old IP address change in the cache become invalid. CA Workload Automation AE does not function properly when a cached IP address is still valid but points to another machine with a CA Workload Automation AE installation on it. To avoid potential loss of productivity in dynamic environments, disable IP address caching.

Note: CA Workload Automation AE verifies the IP address on every network request when IP address caching is disabled. These verifications impact system performance. We recommend that you disable IP address caching only in dynamic environments.

On UNIX, you can disable IP address caching using the EnableIPCaching configuration parameter. For more information about disabling IP address caching on UNIX, see the Administration Guide.

On Windows, you can disable IP address caching using the CA Workload Automation AE Administrator. For information about disabling IP address caching on Windows, see the Online Help.

Setting Job Attribute Environment Variables

You can configure CA Workload Automation AE to automatically set the supported job definition JIL attributes as environment variables.

The agent supports the setting of only the following environment variables based on job definition JIL attribute values:

- __job_name
- __box_name
- __machine
- __run_machine
- __max_exit_success

On UNIX, you can configure this setting using the SetJobAttributeEnvironmentals parameter in the configuration file. For information about setting job definition JIL attributes as environment variables on UNIX, see the Administration Guide.

On Windows, you can configure this setting using the Set Job Attribute Environmentals check box on the Scheduler - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator (on Windows). For information about setting job definition JIL attributes as environment variables on Windows, see the Online Help.

Changes in Release 11.3.5

This section contains the following topics:

Acknowledgments

The acknowledgements for third-party components used by CA Workload Automation AE have been moved from the Release Notes to the acknowledgements.txt file located in the root directory of the installed product.

CA Workload Automation AE Readme

The CA Workload Automation AE Readme is no longer included in the documentation set. The information previously included in the CA Workload Automation AE Readme is included in this document.

Updated autoaggr Command

In Unicenter AutoSys JM r11 and CA Workload Automation AE r11.3, the autoaggr command was used to aggregate statistics into the hourly, daily, weekly, and monthly tables that other programs use to generate reports. In the current release, the autoaggr command generates reports based on the aggregated job, alarm, and scheduler statistics retrieved from the database.

Note: For more information about the autoaggr command, see the Reference Guide.

In the current release, you can aggregate the job, alarm, and scheduler statistics into the database tables in the following ways:

- Manually by using the sendevent command. For more information about the sendevent command, see the Reference Guide.
- Automatically by configuring the AggregateStatistics parameter (on UNIX) or Aggregate Statistics field (on Windows). For more information about these configuration options, see the Administration Guide or the Online Help for CA Workload Automation AE Administrator.

Notes:

- In Unicenter AutoSys JM r11 and CA Workload Automation AE r11.3, the total_latency statistics were collected. In the current release, the total_latency statistics are not collected. Instead, the MAX LATENCY, AVERAGE LATENCY, MAX LAG TIME, and AVERAGE LAG TIME statistics are collected. For more information about the statistics displayed in the reports, see the Reference Guide.
- In Unicenter AutoSys JM r11 and CA Workload Automation AE r11.3, the total_events and total_latency statistics were stored in the jc_jrestart_n and jc_quewait_n database columns respectively. When you upgrade from Unicenter AutoSys JM r11 or CA Workload Automation AE r11.3 to the current release, the values in the jc_jrestart_n database column are copied to the new tc_events_n database column and are then zeroed out. The aggregation process does not generate statistics into the jc_quewait_n, jc_jedit_n, js_activated_n, and js_activated_p database columns and so these database columns are dropped in the current release

Updated autosys_secure command

In the current release, updates to the autosys_secure command allow you to enable and disable external security in batch mode. The addition of the -secadmu option allows you to authenticate autosys_secure with external security as a user with administrative privileges. The addition of the -e parameter allows you to enable external security and generate a CA EEM certificate. The addition of the -n parameter allows you to disable external security and revert to native security.

Note: For more information on the autosys_secure command, see the Reference Guide.

Updated as_info Command

The -C option is added to the as_info command to return the configuration information for all CA Workload Automation AE instances installed on a computer.

Note: For more information about the as_info command, see the Reference Guide.

Updated autoflags Command

The -f option is added to the autoflags command to write the fully qualified host name to standard output.

Note: For more information about the autoflags command, see the Reference Guide.

Updated autosyslog Command

In the current release, updates to the autosyslog command enable you to display the following data:

- The spool file for a job
- The available z/OS job log types and dataset names
- The z/OS job log dataset

To display the spool file, use the S argument with the -T option. To display the available z/OS job log types and dataset names, use the -j parameter with the -z option. To display the z/OS job log dataset, use the -d parameter.

Note: For more information about the autosyslog command, see the Reference Guide.

Updated Highly Available Cluster Environment Options

The current release of CA Workload Automation AE can cooperate with cluster management software to form a clustered server, a clustered database, or a clustered agent. A clustered server is an alternative to high-availability mode and provides a more stable failover solution. A clustered database is an alternative to dual event server mode and is recommended if your database vendor is cluster-aware. A clustered agent complements the load-balancing capabilities of the scheduler and is recommended when you are running jobs that execute client utilities, use shared resources or have high CPU consumption. We recommend setting up a clustered server before you set up a clustered agent. You cannot set up the clustered agent on the same cluster as the clustered server. In the current release, you can also specify a manager host alias for the clustered server.

Note: For more information about setting up a clustered server and a clustered agent, see the UNIX Implementation Guide or the Windows Implementation Guide. For more information about specifying a manager host alias, see the UNIX Implementation Guide or the Online Help.

Alarm Removed

The APP_SERVER_COMM alarm is removed from CA Workload Automation AE.

EP_SHUTDOWN Alarm

The EP_SHUTDOWN alarm is raised when the active scheduler (either the primary scheduler or the shadow scheduler after it takes over processing events while running in high availability mode) is shutting down because of a normal shutdown process or an error condition. This alarm is raised with text containing the role designator, the host, and the time of the scheduler shutdown. If CA Workload Automation AE is configured to send SNMP traps, the scheduler sends two traps with an identifier of 109 (STOP_DEMON) and 521 (EP_SHUTDOWN).

Application and Group Level Security

In previous releases, if you defined the application or group attributes in your job definition, security checks were performed to validate execute access when the job started. However, these security checks were not performed against jobs when they were submitted through the cross-platform interface.

In Release 11.3.5, CA Workload Automation AE also performs application and group level security checks against jobs when they are submitted through the cross-platform interface.

CA EEM Security Policy Authorizations for Jobs

In the current release, CA Workload Automation AE performs more security policy authorizations for jobs than in previous releases. So, you must create additional security policies to authorize users to do the following tasks:

- To define, update, override, or delete a job in a box:
  - If you are defining a job, create a policy in the as-base-jobtype resource class authorizing EXECUTE access to the job_type attribute value that represents a predefined CA Workload Automation AE job type.
  - If you are updating a job, create a policy in the as-job resource class authorizing EXECUTE access to the existing unmodified box_name attribute value to modify the contents of the box with that name.
  - Create a policy in the as-job resource class authorizing EXECUTE access to the box_name attribute value to modify the contents of the box with that name.
  - Create a policy in the as-base-jobtype resource class authorizing EXECUTE access to the predefined CA Workload Automation AE BOX job type to modify the box with the name represented by the box_name attribute.
- To update, override, or delete a job belonging to an application or a group:
  - If you are updating a job, create a policy in the as-appl resource class authorizing WRITE access to the existing unmodified application attribute value.
  - Create a policy in the as-appl resource class authorizing WRITE access to the application attribute value.
  - If you are updating a job, create a policy in the as-group resource class authorizing WRITE access to the existing unmodified group attribute value.
  - Create a policy in the as-group resource class authorizing WRITE access to the group attribute value.

Note: For more information about authorizing users to create, update, or delete objects, see the CA Workload Automation Security Guide.

CA EEM Release 12 Policy Filter Attribute Changes

This topic describes policy filter attribute changes in CA EEM Release 12. Attributes were dropped, deprecated, and added.

Attributes are classified as follows:

- Dropped attributes—Not supported in CA EEM Release 12.
- Deprecated attributes—Compatible with CA EEM r8.4 and Release 12.
- New attributes—Added in CA EEM Release 12. These attributes cannot be used with CA EEM r8.4. Use of the new attributes is recommended only if compatibility with CA EEM r8.4 and Release 12 is not required.

The following attributes were dropped:

- GlobalUser:Parent
- GlobalUser:Path
- User:Parent
- User:Path
- GlobalUserGroup:Parent
- GlobalUserGroup:Path
- GlobalUserGroup:Description
- UserGroup:Parent
- UserGroup:Path
- UserGroup:Description

The following attributes were deprecated:

- DynamicUserGroup:Name
- GlobalUser:GroupMembership
- GlobalUserGroup:GroupMembership
- GlobalUserGroup:Name
- User:GroupMembership
- User:Name
- UserGroup:GroupMembership
- UserGroup:Name

Note: DynamicUserGroup:Name, GlobalUserGroup:Name, and UserGroup:Name will be available in the CA EEM Release 12 CR08 user interface.

The following attributes are new in CA EEM Release 12:

- DynamicUserGroup:GroupName
- GlobalUser:PrincipalName
- GlobalUserGroup:PrincipalName
- UserGroup:GroupName

Deprecated Attribute Syntax

CA EEM 8.4 policies that you import into CA EEM Release 12 can have filter attributes that CA EEM Release 12 does not recognize. You can modify a policy so that its deprecated attributes are compatible with CA EEM r8.4 and Release 12. Alternatively, you can modify a policy so that its deprecated attributes are compatible with CA EEM Release 12 only.

Attributes that have been dropped and some deprecated attributes are not displayed (selectable) for defining or modifying policy filters in CA EEM Release 12. However, if a deprecated attribute is not displayed, you can select the ellipses (…) and type the r8.4 attribute name in the corresponding field.

The table that follows shows deprecated attribute type/value pairs as they are defined in CA EEM policies. The first column shows the CA EEM r8.4 attribute syntax. The second column shows the attribute syntax to use in a CA EEM Release 12 policy for compatibility with CA EEM 8.4, and CA Workload Automation AE r11.3 SP1 and Release 11.3.5. The third column shows the attribute syntax to use in a CA EEM Release 12 policy that is compatible with CA Workload Automation AE Release 11.3.5 and later.

Syntax Used in the r8.4 Filter Definition	r8.4 Syntax to Use in the Release 12 Filter Definition	Release 12 Syntax to Use in the Release 12 Filter Definition
DynamicUserGroup:Name	DynamicUserGroup:Name	DynamicUserGroup:GroupName
GlobalUser:GroupMembership	GlobalUserGroup:Name	GlobalUserGroup:PrincipleName
GlobalUserGroup:GroupMembership	GlobalUserGroup:Name	GlobalUserGroup:PrincipleName
GlobalUserGroup:Name	GlobalUserGroup:Name	GlobalUserGroup:PrincipleName
User:GroupMembership	UserGroup:Name	UserGroup:GroupName
User:Name	GlobalUser:UserName	GlobalUser:PrincipleName
UserGroup:GroupMembership	UserGroup:Name	UserGroup:GroupName
UserGroup:Name	UserGroup:Name	UserGroup:GroupName

Status Changes for Jobs with Cross-Instance Dependencies

The cross-instance interface design now supports reporting status changes to the remote instance for jobs with cross-instance dependencies when those changes result from one of the following:

- The scheduler changes the status of the job when unavailable machine load units, resources or agents prevent a job from running.
- The user changes the status of the job by issuing a sendevent command for one of the following events: JOB_ON_HOLD, JOB_OFF_HOLD, JOB_ON_ICE, JOB_OFF_ICE, JOB_ON_NOEXEC, JOB_OFF_NOEXEC

If the local instance scheduler does not report these status changes to the remote instance scheduler, downstream jobs dependent on the remote jobs may not run when they should, or may run when they should not.

The scheduler internally generates an equivalent CHANGE_STATUS event to report the status change to the remote instance. This helps ensure that the remote scheduler accurately evaluates downstream jobs dependent on the remote jobs, including the job status and exit code conditions of the dependent jobs.

Notes:

- The equivalent CHANGE_STATUS event represents the actual status change that occurs in the local instance, and the event includes text specifying the actual status change. The remote scheduler log records this information.
- For more information about the translated status that the local scheduler sends to the remote instance, see the Administration Guide.
- For more information about cross-instance dependencies, see the User Guide, UNIX Implementation Guide, or the Windows Implementation Guide.

Increase the CA EEM Server List Input in autosys_secure

When you enable external security using the autosys_secure command, you are prompted to enter the CA EEM back end server host name. In Unicenter AutoSys JM r11, you could specify only one CA EEM back end server host name. In CA Workload Automation AE r11.3, you could specify a comma-separated list of CA EEM servers if you configured multiple CA EEM servers for failover. The entire list of CA EEM servers could consist of at most 64 characters.

In the current release, you can specify a comma-separated list of CA EEM servers. The entire list of CA EEM servers can consist of at most 255 characters.

Note: For more information about configuring multiple CA EEM servers for failover, see the CA EEM documentation.

Removed EXECUTE_CATALOG_ROLE Privilege

In the previous release, the Oracle aedbadmin user was granted the EXECUTE_CATALOG_ROLE privilege. In the current release, the EXECUTE_CATALOG_ROLE privilege is not granted to the Oracle aedbadmin user because the aedbadmin user no longer requires it.

Renamed Web Service (WBSVC) to Web Service RPC/Encoded (WBSVC)

The Web Service (WBSVC) job types has been renamed to Web Service RPC/Encoded (WBSVC) in the documentation.

Creating a Forecast Report for Multiple Days

In the current release, you can specify any time frame when creating a forecast report.

You can specify the time frame for a forecast report using the -F and -T attributes of the forecast command. In the previous release, you could specify a time frame up to 24 hours. There are now no limits on the number of days you can specify; however, reports with longer time frames consume more memory and time.

Note: For more information about the forecast command, see the Reference Guide. For more information about how to create a forecast report, see the User Guide.

Job Attribute Environment Variables

The legacy agent supports the setting of job definition JIL attributes as environment variables, which are sourced as part of running a job.

The agent supports the setting of only the following environment variables based on job definition JIL attribute values:

- __job_name
- __box_name
- __machine
- __run_machine
- __max_exit_success

Notes:

You can set these job definitions JIL attributes as environment variables only for command and file watcher jobs.

- The __box_name environment variable is set only if the job is contained within a box.
- The __max_exit_success environment variable is set only for command jobs.

In the current release, you can configure CA Workload Automation AE to automatically set the supported job definition JIL attributes as environment variables using the SetJobAttributeEnvironmentals parameter in the configuration file (on UNIX) or the Set

Job Attribute Environmentals check box on the Scheduler - CA Workload Automation AE Administrator window of CA Workload Automation AE Administrator (on Windows).

Note: For information about setting job definition JIL attributes as environment variables on UNIX, see the Administration Guide. For information about setting job definition JIL attributes as environment variables on Windows, see the Online Help.

Custom job applications that require knowledge of additional job attributes should be rewritten to invoke the GetJobsWithFilter class of the C++ or Java SDK

AUTOPID

The current release does not support setting AUTOPID as an environment variable during job execution.

Notes:

- The AUTOPID environment variable is still valid for jobs that run on the legacy agent.
- For more information about environment variables, see the User Guide, the Reference Guide, or the Online Help.

Exit Code is Returned When a jil Command is Issued

When you issue a jil command, an exit code is returned to indicate the status of the command. A zero (0) exit code indicates success, while a non-zero exit code indicates an error.

Eligibility of Machines with a Factor Value of Zero

In the current release, the scheduler does not disqualify machines with a factor value of zero (0). When all available machines have a factor value of zero (0), the agent selects one of these machines at random and runs the job on that machine.

Note: For more information about the factor attribute in machine definitions, see the Reference Guide and the User Guide.

Configuring the Agent to Behave Like the Legacy Agent

In the current release, if you select the Configure Agent with Legacy Remote Agent Compatibility check box on the Agent Attributes (on UNIX) or Agent Properties (on Windows) panel during the installation, the installer automatically configures the agent to behave like the legacy agent. That is, the job processing behavior of the agent closely matches the job processing behavior of the legacy agent.

If you want to configure the agent to behave like the legacy agent, we recommend that you select the Configure Agent with Legacy Remote Agent Compatibility check box.

If you did not select the Configure Agent with Legacy Remote Agent Compatibility check box during the installation, but later decide to configure the agent to behave like the legacy, you must manually add or edit the compatibility parameters in the agent's agentparm.txt file.

Notes:

- For more information about how the installer configures the agent to work with CA Workload Automation AE, see the UNIX Implementation Guide or the Windows Implementation Guide.
- For more information about configuring the agent to behave like the legacy agent, see the CA Workload Automation Agent for UNIX, Linux, or Windows Release Notes.

New Features in Release 11.3.6

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*.

Changes in Release 11.3.6

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 resources 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

New Features in Release 11.3.6 SP1

This section contains the following topics:

(UNIX) Enabling Core File Creation

On UNIX, core file creation is enabled for the server processes (scheduler and application server) to enhance supportability. Core file creation is enabled only when the server processes are started using the unisvrcntr command or by a root user.

Enabling SSL Communication between CA Workload Automation AE and CA Service Desk

You can enable SSL communication between CA Workload Automation AE and CA Service Desk.

Note: On HP-UX, you cannot enable SSL communication between CA Workload Automation AE and CA Service Desk.

To configure CA Workload Automation AE to work with CA Service Desk using SSL communication, perform the following tasks:

1. Enable SSL communication between CA Workload Automation AE and CA Service Desk.

Note: For information about enabling SSL communication between CA Workload Automation AE and CA Service Desk, see the UNIX Implementation Guide or the Windows Implementation Guide.

2. Specify a HTTPS URL in the ServiceDeskURL parameter in the configuration file (UNIX) or the URL Location field in the Service Desk pane on the Integration - CA Workload Automation AE Administrator window of the Administrator utility (Windows).

New DBMAINT_FAILURE (548) Alarm

The DBMAINT_FAILURE (548) alarm indicates that the DBMaint command failed during automated database maintenance.

New autobcpORAdp.pl Script

On Oracle, you can now use the autobcpORAdp.pl script to synchronize the databases quickly; thereby improving performance.

New status Attribute

The status attribute sets an initial status for a job during insertion. This can prevent jobs from running during the insertion process.

Monitoring Available Disk Space

The agent is now configured to monitor the amount of available disk space and send notifications to warn you when the space is too low. The agent has three disk space warning thresholds:

- Notice—The agent logs a warning notice when the available disk space is less than the size specified in the agent.resourcemon.threshold.disk.warning.notice parameter in the agentparm.txt file. The agent continues to run; it accepts new and eligible pending jobs requests.
- Severe—The agent logs a severe warning when the available disk space is less than the size specified in the agent.resourcemon.threshold.disk.warning.severe parameter in the agentparm.txt file. The agent stops accepting new job requests.
  All jobs that are scheduled to start on this agent are put in a PEND_MACH status.
- Critical—The agent logs a critical warning and shuts down when the available disk space is less than the size specified in the agent.resourcemon.threshold.disk.critical parameter in the agentparm.txt file.

Note: For information about configuring the agent to monitor the available disk space, see CA Workload Automation Agents - 11.3.4.

New MACHINE_DISKTHRESHOLD Alarm

The MACHINE_DISKTHRESHOLD alarm indicates that a disk threshold has been breached on the agent. This alarm is raised when the notice, severe, or critical threshold is breached.

New Machine Status

The Blocked machine status indicates that the agent blocks communication. All jobs that are scheduled to start on the agent are put in a PEND_MACH status.

Changes in Release 11.3.6 SP1

This section contains the following topics:

Aggregate Statistics

In the current release, CA Workload Automation AE aggregates the job, alarm, and scheduler statistics automatically by default. The default value of the AggregateStatistics parameter in the configuration file is now set to 1. Also, the Aggregate Statistics check box in the Scheduler – CA Workload Automation AE window of the Administrator utility is now selected by default.

Note: If you upgrade from Release 11.3.5 or Release 11.3.6 to the current release, the value of the AggregateStatistics parameter in the configuration file is reset to 1.

STATE_CHANGE Event is Issued When a Job Enters the QUE_WAIT, PEND_MACH, or RESWAIT State

When a job is placed in the QUE_WAIT, PEND_MACH, or RESWAIT state, the scheduler now issues a STATE_CHANGE event with an informative message. The event and the associated message are written to the scheduler log and are also displayed in the detailed autorep report that you can generate using the autorep -J jobname -d command.

Updated LOGROLLOVER Parameter

You can now set the LOGROLLOVER parameter to PURGE(x) to purge all log files that are older than the specified number of days at midnight. The default value of the LOGROLLOVER parameter is now set to MIDNIGHT,PURGE(7). All log files that are older than 7 days are purged by default.

Notes:

If you upgrade to the current release, the log files are not purged by default. Use the LOGROLLOVER parameter to specify that all log files that are older than the specified number of days are purged at midnight. For example, to purge log files that are older than 10 days, set the LOGROLLOVER parameter as follows:

LOGROLLOVER=PURGE(10)

For more information about setting the LOGROLLOVER parameter to purge log files, see the Administration Guide.

Email Notifications

If you specify an application or group attribute in your job definition, the application name or the group name is now included in the email notification.

Note: For better readability, view the email notification as plain text. This may require a change to the font used by your email editor.

SNMP Traps

In addition to the alarmName, alarmJobName, alarmText, alarmCode, alarmExitCode, trapDate, and trapMessge values, the SNMP trap now passes the following values:

- alarmMachineName—The name of the machine where the job runs.
- alarmBoxName—The name of the box that includes the job.
- alarmApplicationName—The name of the application that is associated with the job.
- alarmGroupName—The name of the group that is associated with the job.
- alarmRunNum—The run number of the job.
- alarmNtry—The number of times the job was restarted.
- alarmInstanceName—The name of the instance.

Updated as-owner Resource Class

The as-owner resource class controls whether a user has permissions to include the owner attribute in the job definition. In addition, it now also controls whether a user has permissions to the existing job owner value to update, override, or delete any attribute of a job.

Job Name Supports Colon

When you insert, update, override, or delete a job, you can include colons in the job name or the box job name.

Note: Enclose the job name that includes a colon with quotation marks (" ") or precede it with a backslash (\).

Updated EvaluateQueuedJobStarts Parameter

The EvaluateQueuedJobStarts parameter is now updated to support three options for scheduling jobs leaving a queued state.

On UNIX, you can set the EvaluateQueuedJobStarts parameter in the configuration file to 0, 1, or 2.

On Windows, you can select any one of the following options in the Evaluate Queued Job Starts pane under the Options tab on the Scheduler – CA Workload Automation AE Administrator window of the Administrator utility:

- Off
- Skip same day check
- Include same day check

If you set the EvaluateQueuedJobStarts parameter to 0 (UNIX) or Off (Windows), the scheduler immediately starts jobs leaving a queued state.

If you set the EvaluateQueuedJobStarts parameter to 1 (UNIX) or Skip same day check (Windows), the scheduler does not re-evaluate date and time conditions. Jobs that meet their original date and time conditions before entering a queued state start immediately after they leave the queued state unless other starting conditions apply and are not satisfied. Jobs that leave the queued state on a day that is defined in an exclusion calendar or at a time outside their run window do not start and are re-scheduled to their next start time.

If you set the EvaluateQueuedJobStarts parameter to 2 (UNIX) or Include same day check (Windows), the scheduler re-evaluates date conditions but not time conditions.

Jobs that meet their date conditions after leaving a queued state start unless other starting conditions apply and are not satisfied. Jobs that leave the queued state on a day that is defined in an exclusion calendar or at a time outside their run window do not start and are re-scheduled to their next start time.

Note: For more information about configuring CA Workload Automation AE to schedule jobs leaving a queued state, see the Administration Guide or the Online Help.

New Features in Release 11.3.6 SP2

No new features were added in CA Workload Automation AE Release 11.3.6 SP2.

Changes in Release 11.3.6 SP2

This section contains the following topics:

Documentation in the Product Image

The product documentation is no longer included in the product image. You can access the documentation online using this DocOps platform.

Retrieve Information of a Machine Using Web Services

Using web services, you can now retrieve information of a specific machine or multiple machines. For more information, see Managing Machines.

Calendar Name and Description

You can now use the autocal_asc utility to add or modify a description for a calendar. The description can be up to 1024 characters.

The calendar name can now contain up to 64 characters.

Updates to the ON_NOEXEC Feature

In the current release, the following changes are made for the ON_NOEXEC feature:

- JOB_ON_NOEXEC event
  The scheduler processes the JOB_ON_NOEXEC event similar to that of the CHANGE_STATUS event to INACTIVE.
  For example, if you send the JOB_ON_NOEXEC event to a job in a box, the effect is the same as sending the CHANGE_STATUS event to INACTIVE for a job in a box. The job enters the ON_NOEXEC status and the scheduler evaluates the overall box status as if the job entered the INACTIVE status.
  To take the job off the ON_NOEXEC status, you must send the JOB_OFF_NOEXEC event. Sending manual CHANGE_STATUS event does not change the status of the job. To complete the NOEXEC job immediately so that the scheduler evaluates the job as if the job entered the SUCCESS status, send the FORCE_STARTJOB event.
- JOB_OFF_NOEXEC event
  When the scheduler processes the JOB_OFF_NOEXEC event for a job, it places the job in the INACTIVE status. If the job is in a box, the scheduler evaluates the overall box status as the job is entering the INACTIVE status. If you send the JOB_OFF_NOEXEC event to a box, all jobs in the box (including all jobs contained in lower level boxes within the box) are reset to the INACTIVE status.

- Evaluation of downstream dependent jobs
  When you send the JOB_ON_NOEXEC event to a job, the effect is the same as if the job enters the INACTIVE status. The scheduler does not immediately schedule jobs that have a dependency on the NOEXEC job nor does it evaluate their success conditions to success.
  When the job's starting conditions are met and the scheduler sends the BYPASS event, the effect is the same as if the job enters the SUCCESS status with an exit code of 0. The scheduler schedules jobs that have a dependency on the NOEXEC job and evaluates their success conditions to success.

Sending More Detailed Events to External Instances

When a local scheduler sends events to external instances, it populates the Event text field to indicate the action in the local instance that resulted in the external event. The event text can be as follows:

- Job *job name* entered *status*
- Job *job name* was placed ON_HOLD|ON_ICE
- Job *job name* was bypassed and placed ON_NOEXEC
- Job *job name* was not scheduled and was reset to ON_NOEXEC
- Job *job name* was taken off ON_HOLD|ON_ICE|ON_NOEXEC
- Job *job name* was placed in RESTART due to application failure

Adding or Removing Jobs in Boxes

You can add a job into a box by inserting a new job and specifying the box name in the box name attribute value of the inserted job. You can also add a job into a box by modifying the box name in the box name attribute value of an existing job. Similarly, you can remove a job out of a box by deleting the job or by removing the box name in the box name attribute value of the job. When you add or remove jobs in a box, CA Workload Automation AE performs the following actions:

- Modify the job status based on the status of the box
- Send a STARTJOB event to immediately schedule a job that is added to a box in the RUNNING state.
- Send an ALERT event to notify you that the content of the box job is changed.

Note: CA Workload Automation AE sends the ALERT event only when the jobs are removed or added in the box that is in the RUNNING status.

Note: For more information about the actions that CA Workload Automation AE performs on jobs that are added into or removed out of a box, see Box Jobs Overview.

New Features in Release 11.3.6 SP3

This section contains the following topics:

New Job Types

CA WA Advanced Integration for Hadoop lets you integrate with various distributions of Hadoop including Cloudera, Hortonworks, and Apache. You can define the following new job types using CA WA Advanced Integration for Hadoop:

- HDFS (Hadoop Distributed file System)
- Oozie
- Hive
- Sqoop
- Pig

Connection Profiles

A connection profile is a set of attributes that are required for connecting to environments where the job runs. For example, to run a job in the Hadoop environment, you can create a connection profile with the appropriate parameters to connect to the Hadoop cluster, Oozie server, Hive database, or the Sqoop database.

A connection profile lets you save the connection information and you can use the connection profile in the job definition. For example, when you define a Hadoop HDFS job, you can assign a connection profile to it.

Note: For information about the JIL subcommands and attributes that you can use to define, update, and delete connection profiles, see JIL Connection Profile Definitions.

A connection profile applies to the following job types:

- HDFS
- Hive
- Oozie
- Sqoop
- Pig

You can use web services to retrieve information of a specific connection profile or multiple connection profiles. For more information, see Managing Connection Profiles.

New as-connectionprofile Resource Class

The as-connectionprofile resource class and its default CA EEM policy with READ, CREATE, DELETE, EXECUTE, and WRITE access modes is added to control access to a connection profile.

Authenticate a User Using Key Credentials

For robust security, you can authenticate users that run Hadoop (HDFS, Hive, Oozie, Sqoop, or Pig) jobs using key credentials instead of a password.

You can use the autosys_secure command to specify a password or key credentials for a user.

IMPORTANT! You can authenticate only those users that run Hadoop jobs using key credentials.

New Job State

The SUSPENDED (17) job state is added in this release. This job state indicates that the Hadoop Oozie job is suspended.

You can use the suspended monitor or report attribute to specify whether to track the job status event generated when a job changes to the SUSPENDED status. For more information about the suspended attribute, see suspended Attribute -- Specify Whether to Track Job Events When a Jobs Status Changes to SUSPENDED .

New Events

The following events are added in this release:

- RESUMEJOB (I49)–Resumes a Hadoop Oozie job and places it in the RUNNING state. This event is manually generated.
- SUSPENDJOB (148)–Suspends the Hadoop Oozie job and places it in the SUSPENDED state. This event is manually generated.

Use the sendevent command to suspend a Hadoop Oozie job that is in the RUNNING state or to resume a Hadoop Oozie job that is in the SUSPENDED state.

Using web services, you can now issue RESUMEJOB and SUSPENDJOB events. For more information, see Managing Jobs.

New Alarms

The following alarms are added in this release:

- RESUMEJOBFAIL(551)–Indicates that the RESUMEJOB event failed; typically when you send the event with the Hadoop Oozie job not in the SUSPENDED state.
- SUSPENDJOBFAIL (550)–Indicates that the SUSPENDJOB event failed; typically when you send the event with the Hadoop Oozie job not in the RUNNING state.

Changes in Release 11.3.6 SP3

This section contains the following topics:

Updated autosys_secure Command

You can now use autosys_secure (from the command line or using the CA WAAE Security Utility interactive menu) to perform the following tasks:

- Add a regular user with key credentials.
- Change the key credentials of the specified user.
- Display only the list of users with key credentials.
- Display only the list of users with password.

New Features in Release 11.3.6 SP4

This section contains the following topics:

(Oracle only) Support Single Sign-On Wallets with Certificates for Database Access

You can now configure CA Workload Automation AE to use single sign-on wallets with certificates that are present on the file system to access the database. During installation, you can set the database access mode to either password or SSL certificate mode.

The DBAccessMode parameter in the configuration file or the Access Mode field on the Event Server - CA Workload Automation AE Administrator window of the Administrator utility (Windows) displays the access mode that CA Workload Automation AE is using to establish connections to the database.

After you installed CA Workload Automation AE, you can use the switchDBAccessMode.pl script to switch the database access mode from password to SSL certificate mode or vice versa.

Changes in Release 11.3.6 SP4

No features were changed in WAAE Release 11.3.6 SP4.