CA Workload Automation Agent for UNIX, Linux, Windows, or i5/OS

Release Notes

r11.3 SP3

CA Technologies Product References

This document references the following CA Technologies products:

- CA Process Automation
- CA Workload Automation AE
- CA Workload Automation Agent for Application Services (CA WA Agent for Application Services)
- CA Workload Automation Agent for Databases (CA WA Agent for Databases)
- CA Workload Automation Agent for i5/OS (CA WA Agent for i5/OS)
- CA Workload Automation Agent for Informatica (CA WA Agent for Informatica)
- CA Workload Automation Agent for Linux (CA WA Agent for Linux)
- CA Workload Automation Agent for Micro Focus (CA WA Agent for Micro Focus)
- CA Workload Automation Agent for Microsoft SQL Server (CA WA Agent for Microsoft SQL Server)
- CA Workload Automation Agent for Oracle E-Business Suite (CA WA Agent for Oracle E-Business Suite)
- CA Workload Automation Agent for PeopleSoft (CA WA Agent for PeopleSoft)
- CA Workload Automation Agent for Remote Execution (CA WA Agent for Remote Execution)
- CA Workload Automation Agent for SAP (CA WA Agent for SAP)
- CA Workload Automation Agent for UNIX (CA WA Agent for UNIX)
- CA Workload Automation Agent for Web Services (CA WA Agent for Web Services)
- CA Workload Automation Agent for Windows (CA WA Agent for Windows)
- CA Workload Automation CA7 Edition
- CA Workload Automation DE
- CA Workload Automation Desktop Client (CA WA Desktop Client)
- CA Workload Automation ESP Edition
- CA Workload Control Center

Contact CA Technologies

Contact CA Support

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

- Online and telephone contact information for technical assistance and customer services

- Information about user communities and forums

- Product and documentation downloads

- CA Support policies and guidelines

- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

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

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

Contents

Chapter 5: Supported Systems and Requirements 47

Chapter 6: Related Documentation 55

Appendix A: Acknowledgements 77

Chapter 1: Welcome

Welcome to CA Workload Automation Agent for UNIX, Linux, or Windows. This document includes information about changes to existing features, a complete list of fixed issues, supported platform information and system requirements, and known issues for this release, if any. Relevant documentation may also be included for significant fixes or changes.

For the latest version of the 11.3 agent documentation including these Release Notes, visit the following link:

https://supportcontent.ca.com/cadocs/0/CA%20Workload%20Automation%20System%20Agent%20r11%203-ENU/Bookshelf.html

Upgrading the Agent to r11.3 SP3

If you are using CA WA Agent for UNIX, Linux, Windows, or i5/OS r11.3 or higher, you can upgrade to r11.3 SP3 using a patch. To apply the r11.3 SP3 patch, use the current patch utility. The patch installer updates the Java Runtime Environment (JRE) supplied with the agent and provides the same fixes and features as the full installer.

Note: Patch upgrade from Release 7 to r11.3 SP3 is not supported.

You can find the latest CA Workload Automation Agent solutions and patches on CA Support Online:

https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=83c50203-e6a9-427a-afa6-f1dbac9438cf&productID=8075

Upgrade the Agent to r11.3 SP3 on UNIX

If you are using CA WA Agent for UNIX or Linux r11.3 or higher, you can upgrade to r11.3 SP3 using a patch. On AIX systems, remove the cached dynamic libraries from memory as root before you upgrade the agent.

Important! To upgrade the agent on z/Linux, you must have JRE 1.7 SR6 FP1 (31-bit) or higher installed and must set the JRE_HOME environment variable.

Follow these steps:

1. (z/Linux only) Verify that JRE 1.7 SR6 FP1 (31-bit) or higher is installed on the agent computer.

2. (z/Linux only) Set the JRE_HOME environment variable to the JRE 1.7 installed directory.

3. Stop the agent:

    `agent_install_path/cybAgent -s`

    agent_install_path

    > Specifies the agent installation directory.

4. (AIX only) Run the following command as root to remove the cached dynamic libraries from memory:

    `slibclean`

5. Download and unpack the supplied tar.Z file into a temporary location, such as /cybagent/tmp:

    ```
    cd /cybagent/tmp
    uncompress < patch.tar.Z | tar xvf -
    ```

    patch

    > Specifies the name of the patch file.

    The temporary location contains the necessary files for installing the patch.

6. Change the permission of installPatch.sh to 755:

    `chmod 755 installPatch.sh`

7. Apply the patch using the following command:

    `installPatch.sh [-licenseAccepted] agent_install_path patch_file patch_id`

    -licenseAccepted

    > (Optional) Accepts the license agreement. The license agreement is not shown.

    > **Note:** Before applying the patch with the -licenseAccepted option, review the license agreement (license.txt) included with the patch files.

patch_file

> Specifies the archive file that contains the patching files. The file has a TAR extension on UNIX.

patch_id

> Specifies the ID of the patch that is being applied. The ID is usually the name of the file that is downloaded from CA Support Online.

Example: /cybAgent/tmp/installPatch.sh /opt/CA/CAWA_Agent patch_solaris_x86.tar RO55420

8. Start the agent:

`agent_install_path/cybAgent &`

Upgrade the Agent to r11.3 SP3 on Windows

If you are using CA WA Agent for Windows r11.3 or higher, you can upgrade to r11.3 SP3 using a patch.

Follow these steps:

1. Stop the agent:

`agent_install_path\cybAgent -s`

agent_install_path

> Specifies the agent installation directory.

2. Download and unpack the supplied .caz file into a temporary location, such as C:\temp\patch:

`CAZIPXP -u patch.caz`

patch

> Specifies the name of the patch file.

Note: The CAZIPXP utility must reside in the same directory as the .caz file. You can download the CAZIPXP utility from CA Support Online at https://support.ca.com/irj/portal/phpsupcontent?contentID=cb74d332-823b-427e-a6de-811dc2183fb1&fromKBResultsScreen=T.

The temporary folder contains the necessary files for installing the patch.

3. Apply the patch using the following command:

`installPatch.bat [-licenseAccepted] agent_install_path patch_file patch_id`

-licenseAccepted

> (Optional) Accepts the license agreement. The license agreement is not shown.

> **Note:** Before applying the patch with the -licenseAccepted option, review the license agreement (license.txt) included with the patch files.

patch_file

Specifies the archive file that contains the patching files. The file has a ZIP extension on Windows.

patch_id

Specifies the ID of the patch that is being applied. The ID is usually the name of the file that is downloaded from CA Support Online.

Example: installPatch.bat "C:\Program Files\CA\CAWA Agent" patch_windows64.zip RO55422

4. Start the agent:

    agent_install_path\cybAgent -a

Upgrade the Agent to r11.3 SP3 on i5/OS

If you are using CA WA Agent for i5/OS r11.3 or higher, you can upgrade to r11.3 SP3 using a patch.

Important! To upgrade the agent on i5/OS, you must have J2SE 6.0 32-bit installed (Option 11) and must set the JAVA_HOME environment variable to JDK 1.6.

Follow these steps:

1. Verify that JRE 1.6 is installed on the agent computer, for example:

   ```
   java -version
   java version "1.6.0"
   Java(TM) SE Runtime Environment (build pap3260sr13ifix-20130303_02(SR13+IV374
   19))
   IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 OS/400 ppc-32 jvmap3260sr13-201302
   07_01 (JIT enabled, AOT enabled)
   J9VM - 20130114_134867
   JIT  - r9_20130108_31100
   GC   - 20121212_AA)
   JCL  - 20130303_02
   ```

2. Set the JAVA_HOME environment variable to JDK 1.6, for example:

   ```
   JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit
   ```

3. Open a PASE terminal session.

4. Change to the agent installation directory and stop the agent:

   ```
   ./cybAgent -s
   ```

5. Download and unpack the supplied tar.Z file into a temporary location, such as /cybagent/tmp:

   ```
   cd /cybagent/tmp
   uncompress < patch.tar.Z | tar xvf -
   ```

   patch

   Specifies the name of the patch file.

   The temporary location contains the necessary files for installing the patch.

6. Change the permission of installPatch.sh to 755:

   ```
   chmod 755 installPatch.sh
   ```

7. Apply the patch using the following command:

   ```
   installPatch.sh [-licenseAccepted] agent_install_path patch_file patch_id
   ```

   -licenseAccepted

   (Optional) Accepts the license agreement. The license agreement is not shown.

Note: Before applying the patch with the -licenseAccepted option, review the license agreement (license.txt) included with the patch files.

agent_install_path

Specifies the agent installation directory.

patch_file

Specifies the archive file that contains the patching files. The file has a TAR extension on i5/OS.

patch_id

Specifies the ID of the patch that is being applied. The ID is usually the name of the file that is downloaded from CA Support Online.

Example: /cybAgent/tmp/installPatch.sh /opt/CA/CAWA_Agent patch_i5.tar RO61254

8. Change to the agent installation directory and start the agent:

```
./cybAgent
```

Uninstall a Patch

If you updated the agent using the patch installer, you can manually uninstall the most recent patch update. After you uninstall the patch, the agent reverts to the previous version.

Follow these steps:

1. Stop the agent:

    ■ On UNIX:

        agent_install_dir/cybAgent -s

    ■ On Windows:

        agent_install_dir/cybAgent.exe -s

    agent_install_dir

        Specifies the path to the directory where the agent is installed.

2. Make a copy of the agent directory:

    ■ On UNIX:

        cp –r *agent_install_dir agent_install_dir*.backup

    ■ On Windows:

        xcopy *agent_install_dir agent_install_dir*.backup /s

3. Identify the last installed patch in the following directory:

    ■ On UNIX:

        cd *agent_install_dir*/patches

    ■ On Windows:

        cd *agent_install_dir*/patches

4. Copy the contents of the last installed patch to the agent installation directory:

    ■ On UNIX:

        cp –r *agent_install_dir*/patches/*patch_id agent_install_dir*

    ■ On Windows:

        xcopy *agent_install_dir*/patches/*patch_id agent_install_dir* /s

    patch_id

        Specifies the last installed patch file.

5. Delete the last installed patch from the patches directory:

    ■ On UNIX:

        rm –r *agent_install_dir*/patches/*patch_id*

    ■ On Windows, remove *patch_id* from the *agent_install_dir*/patches directory.

The patch is uninstalled successfully. You can now restart the agent.

Chapter 2: Changes to Existing Features

This chapter documents changes made to existing features in CA WA Agent for UNIX, Linux, Windows, or i5/OS r11.3 SP3.

This section contains the following topics:

Alerting the Scheduling Manager When Disk Space Thresholds are Breached

Problem record: SYSAGT-153

If resource monitoring is enabled (agent.resourcemon.enable=true), the agent monitors the amount of available disk space on the agent computer. The agent issues warnings when the following thresholds are breached:

- Notice—The agent logs a warning notice when the disk space reaches this level, but the agent continues to run.

- Severe—The agent logs a severe warning and stops accepting new job requests.

- Critical—The agent logs a critical warning and shuts down.

Currently, these warnings appear in the agent logs and can also be sent as SNMP traps. In this release, you can now configure the agent to send a message to the scheduling manager when these thresholds have been breached.

To alert the scheduling manager when disk space thresholds are breached, set the following parameter to true in the agentparm.txt file:

communication.managerhealthmon_*n*

Indicates whether to alert the scheduling manager that a disk threshold has been breached, where *n* is an integer that corresponds to the scheduling manager being configured. This parameter is applicable if resource monitoring is enabled (agent.resourcemon.enable=true).

true

Sends a message to the scheduling manager when a disk threshold has been breached. A message is also sent when the notice or severe thresholds are resolved. If the critical threshold is breached, the agent sends an emergency shutdown message to indicate the reason for the shutdown.

Note: If the disk situation prevents a proper shutdown, the delivery of the emergency shutdown message is not guaranteed.

false

Does not send a message to the scheduling manager when a disk threshold has been breached.

Default: false

Note: When implemented on the scheduling manager, the scheduling manager can dynamically set this parameter to true.

More information:

Support for AUTOPID and AUTO_JOB_PID

Problem record: SYSAGT-148

The agent now supports the following environment variables that are set for UNIX/Windows (Command) jobs only:

AUTOPID

Displays the process ID of the job agent process that runs a Windows batch file or UNIX script. On UNIX, AUTOPID is set to the parent process ID. On Windows, if a user is specified in the Command job, AUTOPID is set to the process ID of su.exe. If no user is specified in the Command job, AUTOPID is set to the process ID of cybAgent.exe.

AUTO_JOB_PID

(UNIX only) Displays the child process ID spawned by the parent process in a Command job. You can use this environment variable to get the process ID of the UNIX script that the Command job runs.

Support for Converting Java Serialized Objects to Text

Problem record: SYSAGT-146

A payload producing job is a job that produces binary output that is persisted as a serialized Java object. By default, the serialized Java object is stored on the agent computer in the spool directory, using the job name and a numeric suffix as the file name. You can use the output from a payload producing job as an input value to another job, called a payload consuming job. For example, you can set the value of an MBean attribute in a JMX-MBean Attribute Set job to the serialized Java object returned by another job.

Note: For more information about payload producing and payload consuming jobs, see the documentation for your scheduling manager.

In this release, you can now retrieve the contents of Java serialized objects in text format. From the agent, the text format of the Java object can be inspected manually or by an automated test procedure.

To convert the contents of Java serialized objects to text format, set the following parameter to true in the agentparm.txt file:

plugins.object.storage.persistasplaintext

Specifies whether to persist the Java serialized object of a payload producing job in text format in addition to the binary output.

true

Persists the Java serialized object of a payload producing job in text format. The agent converts the Java object to text and outputs it to a text file in the same location as the binary file. The output file of the plain text version has the same name as the binary file, except with a .txt extension.

Notes:

■ This global setting applies to all payload producing jobs. Depending on the number of payload producing jobs, this setting can cause an excess number of files to be created. Alternatively, when supported on the scheduling manager, you can enable this setting at the job-level for specific jobs.

■ SNMP jobs return an array as the Java object. If the array contains only one element, the agent removes the extraneous Java array from the element before converting it to text format. If the array contains more than one element, the agent outputs the entire array in text format. Most SNMP jobs return only one item in the array.

false

Does not persist the Java serialized object of a payload producing job in text format.

Default: false

Note: Currently, you cannot retrieve the text or binary format of Java serialized objects from the scheduling manager. This functionality will be supported in a future release of the scheduling manager.

Searching the Job Log on i5/OS for a Customized Completion Code

Problem record: SYSAGT-145

The agent now supports the ability to search the job log (QPJOBLOG) generated by i5/OS for a customized completion code. When implemented on the scheduling manager, you can specify a text string or regular expression to locate the completion code in the job log.

Note: This feature which will be implemented in a future release of the scheduling manager.

Support for Windows Server 2012 R2

The agent now supports Windows Server 2012 R2.

More information:

Windows Platforms

Changes to Acceptance of License Agreements

To improve the usability of the installer, the following changes have been made to make it easier to accept the license agreement:

- In the GUI-based product installer on Windows, you can now accept the license agreement without scrolling to the end of the license agreement.

- In the console-based product installer, you can accept the license agreement without displaying the full license agreement.

- In the silent installer, you are now required to set a new property ACCEPT_EULA to ACCEPT in the installer properties file. The license agreement is included at the end of the installer properties file.

- In the patch upgrade installer, you can use a new flag -licenseAccepted to bypass the license agreement.

Note: The license agreement (license.txt) in included with the installation package and patch files. Review the license agreement before accepting the license agreement during the installation.

Chapter 3: Known Issues

The chapter details the known issues in CA WA Agent for UNIX, Linux, Windows, or i5/OS r11.3 SP3.

This section contains the following topics:

Resource Temporarily Unavailable Errors on AIX

Valid on AIX

Symptom:

When running jobs on AIX, some of the jobs fail to complete with submission errors (SUBERROR). The job log contains the following error message:

CAWA_E_20039 Cannot fork a new process to execute the job:/usr/bin/ksh, reason:Resource temporarily unavailable.Error code: 11

Solution:

The error can occur because of a memory issue.

Check the maximum number of user processes on your system using the following command:

lsattr -E -l sys0 -a maxuproc

Sample output:

maxuproc 128 Maximum number of PROCESSES allowed per user True

To resolve the issue, we recommend that you increase the number of user processes to 1024 using the following command:

chdev -l sys0 -a maxuproc=1024

Unable to Restart the Agent on z/Linux or AIX

Valid on z/Linux and AIX

Symptom:

After I run UNIX jobs, I stop the agent, but it cannot be restarted. The defaultlog_agent.log contains the following exception and the stack trace:

```
main.MainThread.CybTcpipControllerPlugin.initialize[:283] -
cybermation.library.communications.CybConversationException: Address already in use
…
```

Solution:

The issue occurs when the operating system does not release the agent listening port.

To prevent this issue from occurring on z/Linux, we recommend that you set the following parameter in the agentparm.txt file:

```
oscomponent.closefds=200
```

This parameter causes the agent to close file descriptors, preventing the scripts or binaries of the user from inheriting them.

Note: If this setting does not resolve the issue, increase the value of oscomponent.closefds up to a maximum of 300.

On AIX, oscomponent.closefds is set to 200 by default, but it can be increased to a maximum of 300 if necessary.

Unable to Start Agent after Configuring the Agent for WebLogic

Valid on AIX and z/Linux

Symptom:

When I configure the CA WA Agent for Application Services plug-in for WebLogic, my agent fails to start. The issue occurs when the SNMP connector is enabled on the agent.

Solution:

If you configure the plug-in for WebLogic using the instructions in the *CA Workload Automation Agent for Application Services Implementation Guide*, the following agent parameters will be set:

```
javax.xml.transform.TransformerFactory=com.sun.org.apache.xalan.internal.xsltc.tr
ax.TransformerFactoryImpl
javax.xml.parsers.SAXParserFactory=com.sun.org.apache.xerces.internal.jaxp.SAXPar
serFactoryImpl
javax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.
DocumentBuilderFactoryImpl
```

On agents using IBM JVMs (AIX and z/Linux), these values are incorrect.

Note: The preceding values are correct for agents using non-IBM JVMs (HP-UX, HP-Itanium, Solaris, and Linux).

To correct this problem on AIX and z/Linux

1. Configure the following parameters in the agentparm.txt file to the values shown:

    ```
    javax.xml.transform.TransformerFactory=com.ibm.xtq.xslt.jaxp.compiler.Transfo
    rmerFactoryImpl
    javax.xml.parsers.SAXParserFactory=com.ibm.xml.xlxp.api.jaxp.impl.SAXParserFa
    ctoryImpl
    javax.xml.parsers.DocumentBuilderFactory=org.apache.xerces.jaxp.DocumentBuild
    erFactoryImpl
    ```

2. Start the agent.

i5/OS Job Fails with Spool File Reading Failure

Valid on i5/OS

When running an i5/OS job, the job sometimes fails with the following error message:

```
...MAIN STATE FAILED SetEnd Cmpc(4001) Status(Spool file reading failure. Unable to
retrieve *USER return code. See previous messages in the log.) LStatus(Spool file
reading failure. Unable to retrieve *USER return code. See previous messages in the
log.)...
```

In this issue, the defaultlog_agent.log file located in the agent installation directory contains the following error:

```
Exception reading joblog spool file:
com.ibm.as400.access.ClientAccessDataStream incompatible with
com.ibm.as400.access.NPDataStream
```

This issue is due to a known issue with a third-party library that the agent uses. This issue will be fixed in a future release.

chkusr Utility Not Supported on i5/OS

Valid on i5/OS

The chkusr utility that is provided with the agent is not supported on i5/OS because the standard PAM (Pluggable Authentication Modules) library that chkusr uses is not applicable to the i5/OS environment. This issue will be addressed in a future release.

Resource Monitoring Not Supported in the i5 Agent

The resource monitoring should send an alert to the scheduler when available disk space reaches a threshold defined in agentparm.txt. This feature is not yet supported in the i5 Agent.

Chapter 4: Fixed Issues

The chapter details the issues that have been fixed in CA WA Agent for UNIX, Linux, Windows, or i5/OS r11.3 SP3.

Agent Fails to Use Additional Manager Addresses When a Timeout Error Has Occurred

Problem record: SYSAGT-154

You can configure the agent with multiple scheduling manager addresses for a given manager in the agentparm.txt file. Separate the multiple addresses in the communication.manageraddress_*n* parameter by semi-colons.

If there is a failure using the first address, the agent is designed to try the second address. And so on, until a successful connection is made. However, in one particular failure scenario, the agent starts, but fails to connect to the specified manager. In the transmitter.log, errors indicate that a SocketTimeoutException was received. The agent then logs that it is going to 'sleep' before retrying. The sleep usually defaults to 120000 ms (2 minutes).

The agent continues to retry the address until it is stopped or the manager is reachable. For example, in a failover scenario where the primary manager goes down, the agent after restarting was unable to connect with the backup manager instance.

This issue has been fixed.

Unprintable Characters Display as @ in Reports

Problem record: SYSAGT-151

Valid on CA Workload Automation AE

In some reports on CA Workload Automation AE, unprintable characters such as tabs (\t) are replaced with @.

To address this issue, you can specify the following agent parameter in the agentparm.txt file:

afmtransfer.tab2spaces

Specifies the number of spaces that the agent substitutes for each tab (\t). By default, tabs are replaced with @. You can use this parameter to replace tabs with spaces, so that unprintable tabs are displayed correctly in reports.

Limits: 1-16

Example: 4 (substitute 4 spaces per tab)

Note: If you specify a value less than 1, the parameter is ignored. If you specify a value greater than 16, the parameter is set to 16.

File Watcher Jobs Complete Before the Watch Interval

Problem record: SYSAGT-144

Valid on CA Workload Automation AE

If the monitored file exists in a stable condition for the watch_interval duration when a File Watcher job is started, the job completes immediately. The job does not wait for the interval that is specified in the watch_interval attribute.

In this fix, you can configure the agent to monitor for the file to be stable for the watch_interval duration from the start of the job. If the monitored file does not meet the filter(size/stability) criteria, the agent uses the watch_interval specified in the job definition as the polling interval. The default value for watch_interval is 60 seconds.

You can now configure the behavior of File Watcher jobs using the following agent parameter:

filemon.firstscan.skip

Sets whether the agent skips the first scan of a monitored file. Applies to File Trigger jobs for CREATE, UPDATE, SHRINK, or EXPAND file activity. Also applies to File Watcher jobs when monitoring the existence of a file (not the size).

true

Skips the first scan of the monitored file.

File Watcher Notes:

■   If the file exists in a stable condition when the job runs, the job does not complete immediately after the first scan. The agent waits for the file to be stable for the complete duration of the watch_interval and then completes.

■   The agent uses the watch_interval as the polling interval for all subsequent scans.

false

Uses the first and subsequent scans for the file system activity monitoring.

File Watcher Notes:

■   If the file exists in a stable condition when the job runs, the job completes immediately after the first scan.

■   If the agent does not find the file in the first scan, it uses the watch_interval as the polling interval for all subsequent scans.

Default: false

Note: On CA Workload Automation AE, set this parameter to true for backward compatibility with legacy agents.

Cannot Set Ulimit for Memory

Problem record: SYSAGT-143

Valid on CA Workload Automation AE

When setting the ulimit for all resources to unlimited in a UNIX job, all values are set to unlimited except for memory (process virtual size). The memory resource remains at 32768 and does not change regardless of the hard and soft limits. This issue has been fixed.

chkusr Utility Fails on UNIX

Problem record: SYSAGT-138

When using the chkusr utility that is provided with the agent on UNIX, it sometimes fails with errors similar to the following:

`*** glibc detected *** ./chkusr: free(): invalid pointer: 0x0804ebcc ***`

`...`

This issue has been fixed.

Support for Current Working Directory Relative Path Profile Sourcing

Problem record: SYSAGT-137, SYSAGT-111

You can now configure the agent on UNIX to source job or global profiles relative to the initial working directory when the specified profile does not contain a full path.

You can specify the following agent parameter to configure how the agent sources profiles that do not contain a full path:

oscomponent.profiles.src.location.iwd

Specifies whether the initial working directory is used to source the specified profile when it does not contain a full path.

true

Indicates that the initial working directory is used to source the specified profile when it does not contain a full path.

Note: If the profile is located in a subdirectory under the initial working directory, specify the profile using a relative path: *subdirectory*/my_profile or ./*subdirectory*/my_profile.

false

Indicates that the *installDir*/profiles directory is used to source the specified profile when it does not contain a full path.

Default: false

Note: If the profile path starts with a /, it is considered a full path, for example: /*subdirectory*/my_profile. In this case, the oscomponent.profiles.src.location.iwd setting is ignored.

Example: Assign a Job Profile Without a Path

This example assigns the my_profile profile to a Command job without a path. If oscomponent.profiles.src.location.iwd is set to true, the agent sources the my_profile profile from the initial working directory. Otherwise, the agent sources the my_profile profile from the profiles directory under the agent installation directory.

```
insert_job: test_run
job_type: CMD
machine: unixagent
command: /bin/touch /tmp/test_run.out
profile: my_profile
```

Example: Assign a Job Profile Using a Relative Path

This example assigns the my_profile profile to a Command job using a relative path. If oscomponent.profiles.src.location.iwd is set to true, the agent sources the my_profile profile from the sub_dir directory under the initial working directory. Otherwise, the agent sources the my_profile profile from the profiles/sub_dir directory under the agent installation directory.

```
insert_job: test_run
job_type: CMD
machine: unixagent
command: /bin/touch /tmp/test_run.out
profile: ./sub_dir/my_profile
```

Example: Assign a Job Profile Using a Full Path

This example assigns the my_profile profile to a Command job using a full (absolute) path. The oscomponent.profiles.src.location.iwd setting is ignored.

```
insert_job: test_run
job_type: CMD
machine: unixagent
command: /bin/touch /tmp/test_run.out
profile:  /sub_dir/my_profile
```

Command Job Fails to Run When Environment Variable Ends with a Backslash (Windows only)

Problem record: SYSAGT-136

Valid on CA Workload Automation AE

A command job fails to run on Windows when the job definition contains a manager- or user-specific environment variable whose value ends with a backslash.

For example:

```
AUTOROOT=C:\CA\Workload Automation AE\
```

This issue has been fixed.

Command Job Fails When Using a Glob for Standard Input (Windows only)

Problem record: SYSAGT-135

Valid on CA Workload Automation AE

When you specify the standard input as a global binary large object (glob), command job fails on Windows. This issue has been fixed.

Excessive World Writeable Privileges (UNIX only)

Problem record: SYSAGT-134, SYSAGT-117

The following files that the agent creates on UNIX have excessive world writeable privileges, which can conflict with auditing policies:

- Temporary working shell scripts (CA Workload Automation AE only)

- Standard output and standard error files

- Job logs

- Spool files

To customize the permissions of these files, we highly recommend that you add both of the following parameters to the agentparm.txt file:

oscomponent.defaultfile.permission

Specifies the standard UNIX file permission in octal notation starting with 0. The four-digit octal code specifies the default file access permissions for the following files that the agent creates:

- Temporary working shell scripts (CA Workload Automation AE only)

- Standard output and standard error files

- Job logs

- Spool files

Example: 0600 (grants read and write permissions to the owner, but prevents anybody else from accessing the file)

Notes:

- If oscomponent.defaultfile.permission is not specified, all files the agent creates will have the same permissions as before 11.3 SP1 cumulative 4.

- Temporary working shell scripts are granted execute permissions by the agent regardless of this parameter.

- This parameter does not change the access permission of the spool directory (that is, drwxrwxrwt).

oscomponent.umask

Provides support for the umask command, which turns off (disables) specific permissions that the oscomponent.default.permission parameter allows. The three-digit octal code sets the file mode creation mask (umask) for the following files that the agent creates:

- Temporary working shell scripts (CA Workload Automation AE only)

- Standard output and standard error files

- Job logs

- Spool files

Example: 066 (assuming the default file access permission is 666, this value turns off read and write permissions for the group and others)

Notes:

- If oscomponent.umask is not specified, the default umask of the user that started the agent is used for job logs, spool files, and wrapping scripts.

- For standard output and error files, the default umask of the user that runs the job is used with an exception on AIX and HP-UX. On AIX and HP-UX, the default umask is only used if the umask is set in the user profile.

Notes:

- The oscomponent.defaultfile.permission parameter defines the baseline for file permissions. The umask value further restricts which permissions are allowed to determine the final file permission. The umask value can be set in the oscomponent.umask parameter, the user profile, the job profile, and other sources.

- For job logs, spool files, and wrapping scripts, the agent determines the final file permission using the oscomponent.defaultfile.permission and oscomponent.umask parameters.

- For standard output and error files, the agent determines the final file permission using the oscomponent.defaultfile.permission parameter and the umask value that takes precedence. For example, if you set the umask value in the user profile and job profile, the umask value in the job profile takes precedence. If the umask value is set to 022 in the user profile and 021 in the job profile, the final umask value is 021.

- If you redirect the output of the command in an argument, these parameters do not apply and the file permission depends on the operating system. For example, if you specify the command as "/usr/bin/echo" and the argument as "TEST >> /tmp/TEST.OUTPUT.COMMAND", the file permission of TEST.OUTPUT.COMMAND is unspecified.

- On CA Workload Automation AE, if you get a 4030 completion code, it means that the agent could not read or write to the temporary wrapper script the agent creates. To resolve the error, verify that the combination of oscomponent.defaultfile.permission and oscomponent.umask parameters give the owner at least read and write permission.

Example: Customize the Permissions of the Agent Working Files on CA Workload Automation ESP Edition

In this example, the following agent parameters are set:

```
oscomponent.umask=113
oscomponent.defaultfile.permission=0664
```

When the agent creates the following files, the permissions are set as indicated in parentheses:

- Job logs (-rw-rw-r--)
- Spool files (-rw-rw-r--)

If no user is specified in the job, the permission of the standard output and error files is -rw-rw-r--. If a user is specified in the job with a default umask of 022, the permission of the standard output and error files is -rw-r--r--.

Example: Customize the Permissions of the Agent Working Files on CA Workload Automation AE

In this example, the following agent parameters are set:

```
oscomponent.umask=066
oscomponent.defaultfile.permission=0600
oscomponent.noforceprofile=true
oscomponent.cmdprefix.force=true
oscomponent.profiles.src.delay=true
oscomponent.profiles.global.override=true
```

The job profile has a umask value of 111.

When the agent creates the following files, the permissions are set as indicated in parentheses:

- Temporary working shell scripts (-rwx--x--x)
- Standard output and standard error files (-rw-------)
- Job logs (-rw-------)
- Spool files (-rw-------)

CA WA Agent for Remote Execution Stops Working after Upgrade

Problem record: SYSAGT-132

After you upgrade the agent using the patch utility, CA WA Agent for Remote Execution stops working. During the patch upgrade, the third-party library sinetfactory.jar is replaced by an older version that is included with the agent. This issue has been fixed. The agent now uses the same version of the sinetfactory.jar as CA WA Agent for Remote Execution.

Important! If you install CA WA Agent for Remote Execution on the 11.3 SP1 or 11.3 SP2 agent, the installer prompts to replace the sinetfactory.jar. Enter 'Y' to replace the sinetfactory.jar on that agent, so that you are using the updated JAR file. If you install CA WA Agent for Remote Execution on the 11.3 SP3 agent, the installer prompts to replace the sinetfactory.jar. You do not have to replace the JAR file in this case.

Agent on Solaris Fails to Start or Crashes When Resource Monitoring is Enabled

Problem record: SYSAGT-131

Valid on Solaris

When resource monitoring is enabled on the agent on Solaris, the following issues can occur:

- Agent fails to start. The agent must be started again.
- Agent crashes when the available disk space reaches 0. Resource monitoring must be disabled on the agent.

These issues have been fixed.

Note: For more information on configuring the agent to monitor available disk space, see the *Implementation Guide*.

Agent Hangs During Shutdown (UNIX only)

Problem record: SYSAGT-129, SYSAGT-126

To initiate and track the shutdown, the agent uses PIDs and the ps command, which are prone to error. In rare cases, the shutdown can hang due to the ps command not completing. This issue has been fixed.

Agent Init Script Fails on Solaris

Problem record: SYSAGT-125

Valid on Solaris

The cybagent-$AGENTNAME.init script fails on Solaris due to an unsupported argument -u. This issue has been fixed.

Delays in Job Submission Due to Retrieving Large Spool File

Problem record: SYSAGT-124

Valid on Linux and Solaris

When retrieving a large spool file, the submission of jobs can be delayed, causing the agent to appear to be unresponsive. Jobs are submitted when the spool file processing completes.

To resolve this issue, the following modifications have been made to the agent:

- The thread pool is used for spool file retrieval

- More tracing information is written to the plugin_log_runner.log file when log.level=8 to aid debugging

- Optimization of spool file retrieval to take fewer I/O requests, allowing the agent to complete retrieval requests faster

Cannot Download Files from a Mainframe Server Using USS

Problem record: SYSAGT-123

When trying to download files from a mainframe server using UNIX System Services (USS) for z/OS, the jobs fail with the following error:

```
The system cannot find the path specified
```

In this issue, the agent incorrectly treated PDF files as mainframe data sets instead of as UNIX files. This issue has been fixed.

Incorrect Output Produced in Windows When Using a UNIX-like Emulator

Problem record: SYSAGT-121

When a UNIX-like emulator such as MKS Toolkit is used to execute a shell script, the job produces incorrect output in Windows. In this issue, the shell script performed operations using case-sensitive environment variable names, which the agent incorrectly converted to upper case. This issue has been fixed.

Cannot Comment Out Variable Assignment in Profile File (UNIX only)

Problem record: SYSAGT-120

Valid on CA Workload Automation AE

The agent fails to start if a line in a profile file contains a commented out variable assignment, for example:

`#BL_USER_SPECIFIC_LAB001_VAL_2=user_specific_LAB001_val2`

This issue has been fixed.

Cannot Retrieve Standard Output File When Initial Working Directory is Set to User (UNIX only)

Problem record: SYSAGT-118

When the initial working directory is set to USER (oscomponent.initialworkingdirectory=USER) in the agentparm.txt file, the agent cannot locate the standard output file. This issue has been fixed.

File Watcher Jobs Fail if Watch File Path Contains Spaces or UNC Format

Problem record: SYSAGT-116

Valid on CA Workload Automation AE

When running a File Watcher job, the job fails if the path specified in the watch_file attribute contains spaces, for example:

```
insert_job: fw11
job_type: FW
machine: winagent
watch_file:"C:/Program Files/CA/WA Agent R11.3.2/filewatcher.exe"
owner:Administrator@winagent
```

In addition, the job fails if the path specified in the watch_file attribute is a UNC path, for example:

```
watch_file: \\CYBNT\MyDesktop\notify.txt
```

These issues have been fixed.

User Verify Command Fails (Windows only)

Problem record: SYSAGT-115

If the following parameters are set in the agentparm.txt file, the User verify command fails on CA Workload Automation AE:

```
oscomponent.cmdprefix.force=true
oscomponent.cmdprefix.force.quotes.full=true
oscomponent.lookupcommand=true
```

In addition, Windows jobs fail on other scheduling managers with these settings if no user is specified in the job definition.

This issue has been fixed.

Sending a Signal to a UNIX Process Group

Problem record: SYSAGT-110

In the agentparm.txt file, set oscomponent.wrapper.exec.force=true to enable signal functionality. With this fix, you can now send a signal to an entire process group on UNIX by preceding the signal number with a minus sign (-). For example, you can pause an entire process group by specifying signal -19.

Notes:

- To force the sending of the SIGTERM or SIGKILL signal to a process group, also set oscomponent.sendsig.term.group=true. This parameter is set to false by default.

- You cannot send the signal to PID 0 or 1.

Set oscomponent.wrapper.exec.force=false to enable multiple (chained) command jobs in a job, for example:

```
bin/sleep 10; echo hello
```

Note: With this setting, you cannot send a signal to a job.

oscomponent.sendsig.term.group

Indicates whether the SIGTERM and SIGKILL signals are always sent to the entire process group.

true

Indicates that the SIGTERM and SIGKILL signals are always sent to the entire process group. The signal is sent to the entire group whether the signal number is positive or negative.

false

Indicates that the SIGTERM and SIGKILL signals are not always sent to the entire process group.

Note: On CA Workload Automation AE, this setting ensures full compatibility with the legacy agent and maintains the correct behavior of the sendevent command. For more information about the sendevent command, see the *CA Workload Automation AE Reference Guide*.

Default: false

oscomponent.wrapper.exec.force

Specifies whether the wrapper script the agent generates puts exec in front of the target script or binary. This parameter is applicable if oscomponent.cmdprefix.force is set to true.

true

Indicates that the wrapper script the agent generates puts exec in front of the target script or binary.

false

Indicates that the wrapper script the agent generates does not put exec in front of the target script or binary. Set this parameter to false to enable chained commands, for example, bin/sleep 10; echo hello.

Note: If this parameter is set to false, you cannot send a signal to the job.

Default: false

Failure to Inherit the Associated Solaris Project When Switching Job Owner

Valid on Solaris and AIX

When the agent switches the job owner using setuid, the associated Solaris project that the job owner belongs to is not inherited.

To address this issue, set the following parameter to true in the agentparm.txt file:

oscomponent.native.setuid.enable

Indicates how the job credentials are set based on platform.

true

(On Solaris) Indicates that the job credentials are set using the user ID along with the default Solaris resource management project name.

(On AIX) Indicates that the job credentials are set using the setpcred() system call, which uses the user ID supplied with the job.

Note: On all other platforms, the default value (false) is used.

false

Indicates that the job credentials are set using the setuid() system call, which uses the user ID supplied with the job.

Default: false

Running Windows Command Jobs in CA Workload Automation AE

For backward compatibility running Windows command jobs in CA Workload Automation AE, we recommend that you set the following parameters to true in the agentparm.txt file:

```
oscomponent.cmdprefix.force=true
oscomponent.cmdprefix.force.quotes.full=true
```

oscomponent.cmdprefix.force

> (UNIX) Specifies whether the agent submits the command using a temporary wrapper shell script.
>
> (Windows) Specifies whether the agent submits the command using the Windows command interpreter (cmd.exe).

> **true**
>
>> (UNIX) Indicates that the agent submits the command using a temporary wrapper shell script that the agent generates.
>>
>> (Windows) Indicates that the agent submits the command using cmd.exe. The command is prefixed with "cmd /c" to allow built-in commands such as dir and echo to execute properly.
>>
>> **Note:** Commands that contain embedded blanks in their path (for example, c:\temp\tst one\test.cmd) fail unless oscomponent.cmdprefix.force.quotes.full is also set to true.

> **false**
>
>> (UNIX) Indicates that the agent submits the command by itself without generating the temporary wrapper shell script.
>>
>> (Windows) Indicates that the agent submits the command by itself without using cmd.exe.

> **Default:** false

> **Note:** On CA Workload Automation AE, set this parameter to true for backward compatibility with legacy agents.

oscomponent.cmdprefix.force.quotes.full

Specifies whether the agent wraps the entire command in double quotes before the Windows command interpreter (cmd.exe) runs the command. This parameter is applicable if oscomponent.cmdprefix.force is set to true.

true

Indicates that the agent wraps the entire command in double quotes before cmd.exe runs the command. Set this parameter to true to allow commands that have spaces in their path run without error, for example:

```
"C:\ Program Files (x86)\command.bat" "C:\ Program Files (x86)\input-file"
```

Notes:

■ Commands that contain embedded blanks in their paths succeed, for example: C:\Program Files\program.exe.

■ Commands with arguments fail if the entire command, including arguments, is quoted, for example: "C:\tools\program.exe arg1 arg2".

false

Indicates that the agent does not wrap the entire command in double quotes before cmd.exe runs the command.

Notes:

■ Commands that contain embedded blanks in their paths fail, for example: C:\Program Files\program.exe.

■ Commands with arguments succeed if the entire command, including arguments, is quoted and the path does not contain embedded spaces, for example: "C:\tools\program.exe arg1 arg2".

Default: false

Note: On CA Workload Automation AE, set this parameter to true for backward compatibility with legacy agents.

Example: Run a Command Using cmd.exe

In this example, you run the following command in a Windows job:

```
c:\temp\tst one\test.cmd one two
```

Initially, the following agent parameters are set:

```
oscomponent.cmdprefix.force=true
oscomponent.cmdprefix.force.quotes.full=false
```

As a result, the system executes the following command, resulting in a failed job:

```
C:\Users\userID>"C:\Windows\SYSTEM32\cmd.exe" /c c:\temp\tst one\test.cmd
'c:\temp\tst' is not recognized as an internal or external command, operable program
or batch file.
```

To resolve this issue, set both parameters to true:

```
oscomponent.cmdprefix.force=true
oscomponent.cmdprefix.force.quotes.full=true
```

As a result, the system encloses the entire command that is submitted to cmd.exe in quotes, resulting in a successful job:

```
C:\Users\userID>"C:\Windows\SYSTEM32\cmd.exe" /c "c:\temp\tst one\test.cmd" one two
```

More information:

Configure the Agent for Legacy Remote Agent on Windows

Chapter 5: Supported Systems and Requirements

This section contains the following topics:

UNIX and Linux Platforms

CA WA Agent for UNIX or Linux r11.3 SP3 supports the following platforms:

Notes:

- These operating environments have been certified at the time of General Availability (GA). Additional operating environments may be certified post GA. For current information regarding operating environment support, visit the CA Workload Automation Agent Product page at the following link:

    https://support.ca.com/irj/portal/prddtlshome?productID=8075

    From the Product Status section, follow the CA Workload Automation Compatibility Information link. Then follow the CA Workload Automation Agent link.

- The agent has native 64-bit support on AIX, HP-UX Itanium, and Linux.

- You can run a 32-bit agent on a 64-bit operating system, as long as the 32-bit libraries are installed.

- You can migrate from a 32-bit Release 7 agent to a 64-bit r11.3 SP3 agent on the same operating system. For more information about migration, see the *Implementation Guide*.

Platform	Supported Versions	OS Architecture	Agent Architecture	Notes
AIX	6.1 7.1	32/64-bit	32/64-bit	On AIX 6.1, install the latest fix pack from IBM: http://www-933.ibm.com/support/fixcentral

Platform	Supported Versions	OS Architecture	Agent Architecture	Notes
HP-UX PA-RISC	11i v1 (11.11) 11i v2 (11.23) 11i v3 (11.31)	32/64-bit	32-bit	On HP-UX PA-RISC 11.11, install the latest Java and JRE patches from HP: ■ http://ftp.hp.com/pub/softlib/hpuxjava-patchinfo/g-11.11-6.0-1111.0812.html ■ https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJDKJRE60 We recommend that you increase the number of threads per process on the HP-UX system. Otherwise, the following error can occur when multiple jobs are run at the same time: java.lang.OutOfMemoryError: unable to create new native thread To increase the number of threads per process, increase the value of the max_thread_proc parameter on the HP-UX system. We recommend that you set it to 1024. On HP-UX PA-RISC 11.23, install the latest Java patches from HP: http://ftp.hp.com/pub/softlib/hpuxjava-patchinfo/g-11.23-6.0-1123.1012.html
HP-UX Itanium	11i v1 (11.11) 11i v2 (11.23) 11i v3 (11.31)	64-bit	64-bit	On HP-UX Itanium 11.23, install the latest Java and JRE patches from HP: ■ http://ftp.hp.com/pub/softlib/hpuxjava-patchinfo/g-11.23-6.0-1123.1012.html ■ https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJDKJRE60
Linux	RHEL 5 or 6 SUSE Linux Enterprise Server 10 or 11	X64 or x86 32/64-bit	32/64-bit	Before installing the agent on Linux, install the following: ■ libstdc++33-32bit or compat-libstdc++ 32-bit (depending on availability) ■ glibc-2.4 32-bit
Solaris	10 or 11	SPARC 32/64-bit x86 32/64-bit	32-bit	

Platform	Supported Versions	OS Architecture	Agent Architecture	Notes
z/Linux	RHEL 5 or 6 SUSE Linux Enterprise Server 10 or 11	31/64-bit	32-bit	Before installing the agent on z/Linux, install the following: ■ libstdc++33-32bit or compat-libstdc++ 32-bit (depending on availability) ■ glibc-2.4 32-bit

UNIX and Linux System Requirements

The following table lists the minimum and recommended hardware requirements and software requirements for the agent.

Notes:

■ Based on your workload volume and environment, you can require additional disk space.

■ A Java Runtime Environment (JRE) runs the agent. The JRE is supplied with the agent for all platforms except z/Linux. For z/Linux, install the required JRE version.

Important! Do not replace the JRE that comes with the agent.

Platform	Minimum Disk Space Required	Minimum Temporary Disk Space for Installation	JRE Version	Notes
AIX	300 MB	500 MB	JRE 1.7 SR6 FP1	
HP-UX PA-RISC	300 MB	500 MB	JRE 1.6 update 22	
HP-UX Itanium	300 MB	500 MB	JRE 1.7 update 9	
Solaris	300 MB	500 MB	JRE 1.7 update 51	
Linux	300 MB	500 MB	JRE 1.7 update 51	
z/Linux			JRE 1.7 SR6 FP1, or higher (31-bit)	The JRE is not supplied with the agent.

Windows Platforms

CA WA Agent for Windows r11.3 SP3 supports the following Windows platforms:

Notes:

■ These operating environments have been certified at the time of General Availability (GA). Additional operating environments may be certified post GA. For current information regarding operating environment support, visit the CA Workload Automation Agent Product page at the following link:

https://support.ca.com/irj/portal/prddtlshome?productID=8075

From the Product Status section, follow the CA Workload Automation Compatibility Information link. Then follow the CA Workload Automation Agent link.

■ The agent has native 64-bit support on Windows.

■ The native CA WA Agent for Windows r11.3 fully exploits 64-bit technology with optimal performance running on the 64-bit version of the operating system. Earlier releases of the agent running 32-bit mode, while supported, have inherent limitations on 64-bit Windows. We recommend, if running the agent on the Windows 64-bit version of the operating system, that you match the native agent to run in 64-bit mode.

■ You can migrate from a 32-bit Release 7 agent to a 64-bit r11.3 SP3 agent on the same operating system. For more information about migration, see the *Implementation Guide*.

Platform	Supported Versions	OS Architecture	Agent Architecture
Windows	Server 2008	32/64-bit	32/64-bit
	Server 2008 R2 SP2	64-bit	64-bit
	7	32/64-bit	32/64-bit
	8	32/64-bit	32-64-bit
	Server 2012	64-bit	64-bit
	Server 2012 R2	64-bit	64-bit

Windows System Requirements

The following table lists the minimum and recommended hardware requirements and software requirements for the agent.

Notes:

■ Based on your workload volume and environment, you can require additional disk space.

■ A Java Runtime Environment (JRE) runs the agent. The JRE is supplied with the agent.

Important! Do not replace the JRE that comes with the agent.

Platform	Minimum Disk Space Required	Minimum Temporary Disk Space for Installation	JRE Version
Windows	300 MB	500 MB	JRE 1.7 update 51

i5/OS Platforms

The agent supports any i5/OS or i5 system that supports i5/OS, Version V5R4M0, or higher.

Note: Ensure that IBM PTF SI27705 is installed on V5R4MO systems.

i5/OS System Requirements

CA Workload Automation Agent for i5/OS requires the following environments:

- J2SE 6.0 32-bit (Option 11)

  Note: To install the agent on i5/OS systems, you must have J2SE 6.0 32-bit installed and the JAVA_HOME environment variable must be set to JDK 1.6, for example:

  JAVA_HOME= /QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit

- PASE (5722SS1 - Portable Application Solutions Environment, option 33)

- TCP/IP (5722-TC1) or TCP/IP (5722-AC1, AC2 or AC3) if you are using the agent to run SSL FTP workload

- Installation of the latest i5/OS CUM distribution

- The required group PTF levels for your i5/OS system

  For V5R4, the required minimum group PTF levels are as follows:

Group PTF	Level	Description
SF99540	9321	CUMULATIVE PTF PACKAGE C9321540
SF99539	118	Group Hiper PTF
SF99291	22	Java Group PTF
SF99315	13	TCP/IP Group PTF

For V6R1, the required minimum group PTF levels are as follows:

Group PTF	Level	Description
SF99610	10047	CUMULATIVE PTF PACKAGE C0047610
SF99609	57	Group Hiper PTF
SF99562	11	Java Group PTF
SF99354	5	TCP/IP Group PTF

For V7R1, the required minimum group PTF levels are as follows:

Group PTF	Level	Description
SF99710	11116	CUMULATIVE PTF PACKAGE C1116710
SF99709	46	Group Hiper PTF
SF99572	6	Java Group PTF
SF99367	5	TCP/IP Group PTF

Chapter 6: Related Documentation

This chapter includes documentation updates made as a direct result of the functionality changes and fixed issues in this service pack.

This section contains the following topics:

Install the JRE on z/Linux

If you are installing the agent on z/Linux systems, you require the following Java Runtime Environment (JRE) version to be installed on your system:

JRE 1.7 SR6 FP1, or higher

Note: The supported JRE is 31-bit. The 64-bit JRE is not supported.

Set the PATH Environment Variable on z/Linux

When you have the required JRE installed on your z/Linux system, set the PATH environment variable as follows:

export PATH=*java_binary_location*:$PATH

java_binary_location

Specifies the full path to the Java binary located in the JRE directory.

Example: export PATH=/usr/java7/jre/bin:$PATH

Install the Agent on UNIX Using an Interactive Program

You can install the agent using an interactive program that lets you change and review your settings before starting the installation process. The installation program installs a packaged Java Virtual Machine (JVM) for the agent.

Follow these steps:

1. Log in as root.

2. Copy the setup file from the product CD or download a zip file from the CA Support Online website, found at http://ca.com/support.

3. Copy or FTP the setup file to the target system and directory.

4. Obtain execute permission for the setup file using the following command:

   chmod +x

5. (Optional) Set the IATEMPDIR environment variable to override the system temp directory:

   IATEMPDIR=/opt/CAWA/*tempdir*
   export IATEMPDIR

   tempdir

   Specifies the path to a temporary directory the agent installation program uses during the installation process.

6. Start the installation using the following command:

   ./setup.bin -i console

7. Press Enter.

   You are prompted to accept the license agreement.

8. Press Enter to display the license agreement or enter **2** to accept the license agreement without displaying it.

   Note: Before you skip the license agreement, review the license agreement (license.txt) included with the installation package.

   If you chose to display the license agreement, enter **y** at the end of the license agreement to accept it.

9. Continue with the installation by entering the required information.

   Notes:

   ■ For z/Linux systems, you must have the required JRE installed and the PATH environment variable set to complete the installation.

   ■ To comply with U.S. Government encryption standard FIPS 140-2, select AES when you are prompted for the cipher algorithm.

10. Review your selections. To return to a previous option, type **back**.

11. Press Enter to exit the installation program.

The agent is installed and the settings are stored in the agentparm.txt file that is located in the agent installation directory.

Notes:

■ If you are installing the agent on a Linux computer that is SELinux enabled, a warning message appears. Change the default security context for IDL.

■ If you have problems with the agent installation, you can display debugging information for troubleshooting purposes.

Install the JRE on i5/OS

To install the agent on i5/OS systems, you must have J2SE 6.0 32-bit installed (Option 11), for example:

```
java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pap3260sr13ifix-20130303_02(SR13+IV374  19))
IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 OS/400 ppc-32 jvmap3260sr13-201302
07_01 (JIT enabled, AOT enabled)
J9VM - 20130114_134867
JIT  - r9_20130108_31100
GC   - 20121212_AA)
JCL  - 20130303_02
```

Change the JAVA_HOME Environment Variable on i5/OS

If you are installing the agent on an i5/OS system and the JAVA_HOME environment variable is not set to JDK 1.6, set JAVA_HOME as follows:

```
JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit
```

Install the Agent Using an Interactive Program on i5/OS

You can install the agent using an interactive program that lets you change and review your settings before starting the installation process. The installation program installs a packaged Java Virtual Machine (JVM) for the agent.

Note: You can also use a silent installation program which lets you automate the installation. When you have multiple agents to install, a silent installation is useful.

Follow these steps:

1. Copy the setup file from the product CD or download a zip file from the CA Support Online website, found at http://ca.com/support.

2. Log on to the i5/OS system using the i5/OS user profile you created for the agent.

3. FTP the setup file in binary mode to a directory in the root file system.

4. Open a PASE terminal session.

   Note: Alternatively, you can install the agent using SSH. When installing the agent using SSH, verify that the OpenSSH server (SSHD) is started using STRTCPSVR SERVER(*SSHD). For more information about starting the OpenSSH server on V6R1 machines and above, search the IBM documentation.

5. Change to the directory where the setup file was uploaded.

6. Enter the following command:

   `export JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit`

   The default JRE is set to Java 6.0.

7. Start the installation using the following command:

    ```
    java –jar setup.jar
    ```

    Note: If you are using a 5250 emulator to install the agent and want to configure the agent FTP server, use the –DTerminal.CanMask=false option. The 5250 emulator does not allow the masking of the password that is required when configuring the FTP server. In this case, type the following command to start the installation:

    ```
    java –DTerminal.CanMask=false –jar setup.jar
    ```

    You are prompted to accept the license agreement.

8. Press Enter to display the license agreement or enter **2** to accept the license agreement without displaying it.

    Note: Before you skip the license agreement, review the license agreement (license.txt) included with the installation package.

    If you chose to display the license agreement, enter **y** at the end of the license agreement to accept it.

9. Continue with the installation by entering the required information.

    Note: To comply with U.S. Government encryption standard FIPS 140-2, select AES when you are prompted for the cipher algorithm.

10. Review your selections. To return to a previous option, type **back**.

11. Press **Enter** to exit the installation program.

    The agent is installed and the settings are stored in the agentparm.txt file that is located in the agent installation directory.

Silent Installer Properties

The following property was added:

ACCEPT_EULA

Indicates whether to accept or reject the license agreement.

ACCEPT

Accepts the license agreement.

REJECT

Rejects the license agreement. The installation is aborted.

Default: REJECT

Note: The license agreement is not shown during the silent installation. Before you set ACCEPT_EULA to ACCEPT, review the license agreement that is included at the end of the installer properties file.

Silent Installer Example

The following example shows the property settings for installing an agent using the silent installer.

Example: Configuring the Installer Properties File

The installer properties file in this example installs an agent that is named AGENT2 on a UNIX system in the agent_solaris_aes directory. The agent uses port 34520 for communication with the scheduling manager named manager1 that has an IP address ::FFFF:192.168.00.00 and uses port 8507. Local security for AGENT2 is enabled. The agent uses the AES cipher algorithm. The FILE1.txt file contains the environment variables that the agent and scheduling manager use. More spool-related parameters are appended at the end of the agentparm.txt file as listed in the additional_agentparm.txt file.

Note: The license agreement is not shown during the silent installation. To accept the license agreement, set ACCEPT_EULA to ACCEPT. By default, the installation is aborted. A copy of the license agreement is included at the end of the installer properties file.

```
ACCEPT_EULA=ACCEPT
USER_INSTALL_DIR=/u1/build/CA/agent_solaris_aes
AGENT_INFO_1=AGENT2
AGENT_INFO_2=34520
NUM_MANAGER_1=1
MANAGER_1_INFO_1=manager1
MANAGER_1_INFO_2=::FFFF:192.168.00.00
MANAGER_1_INFO_3=8507
STRONG_ENCRYPTION_CIPHER=AES
STRONG_ENCRYPTION_KEYGEN=0x0102030405060708010203040506070708
LOCAL_SECURITY=on
NUM_MANAGER_VARS_2=1
MANAGER_VARS_1_INFO_1=MANAGER1_VAR
MANAGER_VARS_1_INFO_2=C:\\MANAGER_1\\FILE1.TXT
NUM_USER_VARS_2=1
USER_VARS_1_INFO_1=USER1
USER_VARS_1_INFO_2=C:\\USER1\\FILE1.TXT
JOBLOG=true
RAW_DATA=/usr/home/joe/additional_agentparm.txt
```

The additional_agentparm.txt file that is specified in the RAW_DATA property contains the following parameters:

```
runnerplugin.spool.clean.enable=true
runnerplugin.spool.expire=50000
runnerplugin.spool.sleep=20000
```

How to Remove the Agent

You can remove an agent when you no longer require it.

To remove the agent, follow these steps:

1. Uninstall the agent:

   ■ On UNIX

   ■ On Windows using the uninstall program (see page 61)

   ■ On Windows silently (see page 62)

2. Remove the agent from the scheduling manager.

   For detailed instructions to remove the agent from the scheduling manager, see the documentation for your scheduling manager.

Uninstall the Agent on Windows Using the Uninstall Program

You can uninstall the agent after you have upgraded it from a previous release, or when you want to remove the agent from your system.

Follow these steps:

1. Verify that all workload is complete.

2. Stop the agent.

3. Launch the uninstall program using Add/Remove Programs (Uninstall a program), similar to other Windows applications.

   The Uninstall CA Workload Automation Agent R11.3 dialog opens.

4. Click Uninstall.

   The product files are deleted and the agent is uninstalled.

5. Click Done to close the dialog.

Uninstall the Agent on Windows Silently

You can uninstall the agent after you have upgraded it from a previous release, or when you want to remove the agent from your system. To uninstall the agent silently, run the uninstall executable from the command prompt.

Follow these steps:

1. Verify that all workload is complete.

2. Stop the agent.

3. Open a command prompt.

4. Run the following command:

   "*agent_install_dir*\UninstallData\Uninstall WA Agent R11.3.exe" -i silent

   agent_install_dir

   Specifies the path to the directory where the agent is installed.

Note: The agent installation directory and any files that were created after the initial installation (such as agent logs) are not removed.

Configure Communication with a Scheduling Manager

You can change your scheduling manager connection information or can add a connection to a different scheduling manager. If you use the agent with two scheduling managers that require different socket types for communication, specify a main and auxiliary socket for the agent.

To configure communication with a scheduling manager, configure the following parameters on the agent:

communication.inputport

Specifies the main port number the agent uses to listen for incoming messages from the scheduling manager. You need this port when you configure the scheduling manager to work with the agent.

Default: 7520

Limits: 1024-65534

communication.inputport.aux

Specifies the optional auxiliary port number the agent uses to listen for incoming messages from the scheduling manager.

communication.managerid_*n*

Specifies the name of the scheduling manager instance that the agent works with, where *n* is an integer that corresponds to the scheduling manager being configured.

Default: CENTRAL_MANAGER

Example: MYSERVER

communication.manageraddress_*n*

Specifies the address of the scheduling manager that the agent works with, where *n* is an integer that corresponds to the scheduling manager being configured. This value corresponds to the IP address in the connection details for the scheduling manager. You can specify a list of addresses for the scheduling manager.

Example: 172.24.36.107 (IPv4) or 0:0:0:0:0:FFFF:192.168.00.00 (IPv6)

Notes:

■   You can specify a DNS name instead of the IP address for the scheduling manager. However, your agent computer must always be able to resolve the DNS name. If there is a DNS outage and your agent computer cannot resolve DNS names, the agent cannot communicate with the scheduling manager.

■   If the scheduling manager address never changes, enter the DNS name for the scheduling manager in the hosts file for your agent computer. This entry ensures that the IP address can be resolved after DNS disruptions.

communication.managerport_*n*

Specifies the port that the scheduling manager listens on for communication from agents, where *n* is an integer that corresponds to the scheduling manager being configured. This value corresponds to the port number in the connection details for the scheduling manager.

Default: 7507

Limits: 1024-65534

communication.managerhealthmon_*n*

Indicates whether to alert the scheduling manager that a disk threshold has been breached, where *n* is an integer that corresponds to the scheduling manager being configured. This parameter is applicable if resource monitoring is enabled (agent.resourcemon.enable=true).

true

Sends a message to the scheduling manager when a disk threshold has been breached. A message is also sent when the notice or severe thresholds are resolved. If the critical threshold is breached, the agent sends an emergency shutdown message to indicate the reason for the shutdown.

Note: If the disk situation prevents a proper shutdown, the delivery of the emergency shutdown message is not guaranteed.

false

Does not send a message to the scheduling manager when a disk threshold has been breached.

Default: false

Note: When implemented on the scheduling manager, the scheduling manager can dynamically set this parameter to true.

communication.monitorobject_*n*

Specifies the monitor object for the scheduling manager that is used in agent alive ping.

communication.socket_*n*

Defines the socket type the agent and scheduling manager use for communication, where *n* is an integer starting at one that corresponds to the scheduling manager being configured. The following socket types are available:

■ plain

■ dylan

Default: plain

Note: CA Workload Automation DE does not require this parameter.

communication.receiver.socket.main

Specifies the type of socket the agent uses for its main port. The value of this parameter must be different from the communication.receiver.socket.aux parameter. You can specify the following socket types:

■ plain

■ dylan

Default: plain

Note: CA Workload Automation DE does not require this parameter.

communication.receiver.socket.aux

Specifies the type of socket the agent uses for its auxiliary port. The value of this parameter must be different from the communication.receiver.socket.main parameter. You can specify the following socket types:

■ plain

■ dylan

Note: CA Workload Automation DE does not require this parameter.

Note: You can configure the agent to work with multiple scheduling managers by adding more definitions in the agentparm.txt file.

Example: Configure the Agent to Communicate with a Scheduling Manager

In this example, the following configuration parameters are set in the agentparm.txt file for a scheduling manager running under the instance "ACE" at address 130.200.146.134. The scheduling manager listens for incoming messages from the agent on port 49155:

```
communication.inputport=7520
communication.managerid_1=ACE
communication.manageraddress_1=130.200.146.134
communication.managerport_1=49155
communication.monitorobject_1=CAEWA_AGENT/AGENTMON1.0/MAIN
communication.receiver.socket.main=plain
communication.socket_1=plain
```

Configure the Agent to Monitor Available Disk Space

You can configure the agent 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 disk space reaches this level, but the agent continues to run.

- Severe—The agent logs a severe warning and stops accepting new job requests.

- Critical—The agent logs a critical warning and shuts down.

The agent logs the notice, severe, and critical warning messages in the runner_os_component.log and nohup.stderr logs. You can configure the agent to send SNMP traps or alert the scheduling manager when disk thresholds are breached.

To configure the agent to monitor available disk space, configure the following parameters on the agent:

agent.resourcemon.enable

Indicates whether to monitor disk space usage and report errors when thresholds are breached.

true

Enables resource monitoring. You can configure the amount of available disk space the agent monitors at each threshold and can send notifications when the space is too low.

false

Disables resource monitoring.

Default: false

Notes:

- To send SNMP traps when the disk thresholds are breached, configure the agent to connect with an SNMP manager.

- To alert the scheduling manager when a disk threshold has been breached, also set communication.managerhealthmon_*n* to true.

agent.resourcemon.threshold.disk.warning.notice

Specifies the amount of disk space that is required before the agent logs a warning notice. The agent continues to run and accept new job requests. This parameter is applicable if agent.resourcemon.enable is set to true. This parameter uses the following syntax:

size[B|K|M|G]

size

Specifies the amount of disk space in bytes (B), kilobytes (K), megabytes (M), or gigabytes(G).

Default: 21M

agent.resourcemon.threshold.disk.warning.severe

Specifies the amount of disk space that is required before the agent logs a severe warning and stops accepting new job requests. This parameter is applicable if agent.resourcemon.enable is set to true. This parameter uses the following syntax:

size[B|K|M|G]

size

Specifies the amount of disk space in bytes (B), kilobytes (K), megabytes (M), or gigabytes (G).

Default: 20M

Note: The agent resumes accepting new job requests when the available disk space is greater than the size specified by this parameter.

agent.resourcemon.threshold.disk.critical

Specifies the amount of disk space that is required before the agent logs a critical warning and shuts down. This parameter is applicable if agent.resourcemon.enable is set to true. This parameter uses the following syntax:

size[B|K|M|G]

size

Specifies the amount of disk space in bytes (B), kilobytes (K), megabytes (M), or gigabytes (G).

Default: 10M

Configure the Agent for Monitoring File Activity

Depending on the type of file activity the agent monitors, you can configure the following parameters to skip the first scan of a monitored file:

filemon.firstscan.skip

Sets whether the agent skips the first scan of a monitored file. Applies to File Trigger jobs for CREATE, UPDATE, SHRINK, or EXPAND file activity. Also applies to File Watcher jobs when monitoring the existence of a file (not the size).

true

Skips the first scan of the monitored file.

File Watcher Notes:

- If the file exists in a stable condition when the job runs, the job does not complete immediately after the first scan. The agent waits for the file to be stable for the complete duration of the watch_interval and then completes.

- The agent uses the watch_interval as the polling interval for all subsequent scans.

false

Uses the first and subsequent scans for the file system activity monitoring.

File Watcher Notes:

- If the file exists in a stable condition when the job runs, the job completes immediately after the first scan.

- If the agent does not find the file in the first scan, it uses the watch_interval as the polling interval for all subsequent scans.

Default: false

Note: On CA Workload Automation AE, set this parameter to true for backward compatibility with legacy agents.

filemon.update.firstscan.skip

Sets whether the agent skips the first scan of a monitored file for UPDATE activity with no change. Applies to only File Trigger jobs.

true

Skips the first scan on update of the monitored file.

false

Uses the first and subsequent scans for the file system activity monitoring.

Default: false

Note: Set this parameter to true to emulate R7 agent behavior.

Change the Default Permissions of the Files Created by the Agent

Problem record: SYSAGT-134, SYSAGT-117

The following files that the agent creates on UNIX have excessive world writeable privileges, which can conflict with auditing policies:

- Temporary working shell scripts (CA Workload Automation AE only)

- Standard output and standard error files

- Job logs

- Spool files

To customize the permissions of these files, we highly recommend that you add both of the following parameters to the agentparm.txt file:

oscomponent.defaultfile.permission

Specifies the standard UNIX file permission in octal notation starting with 0. The four-digit octal code specifies the default file access permissions for the following files that the agent creates:

- Temporary working shell scripts (CA Workload Automation AE only)

- Standard output and standard error files

- Job logs

- Spool files

Example: 0600 (grants read and write permissions to the owner, but prevents anybody else from accessing the file)

Notes:

- If oscomponent.defaultfile.permission is not specified, all files the agent creates will have the same permissions as before 11.3 SP1 cumulative 4.

- Temporary working shell scripts are granted execute permissions by the agent regardless of this parameter.

- This parameter does not change the access permission of the spool directory (that is, drwxrwxrwt).

oscomponent.umask

Provides support for the umask command, which turns off (disables) specific permissions that the oscomponent.default.permission parameter allows. The three-digit octal code sets the file mode creation mask (umask) for the following files that the agent creates:

- Temporary working shell scripts (CA Workload Automation AE only)

- Standard output and standard error files

- Job logs

- Spool files

Example: 066 (assuming the default file access permission is 666, this value turns off read and write permissions for the group and others)

Notes:

- If oscomponent.umask is not specified, the default umask of the user that started the agent is used for job logs, spool files, and wrapping scripts.

- For standard output and error files, the default umask of the user that runs the job is used with an exception on AIX and HP-UX. On AIX and HP-UX, the default umask is only used if the umask is set in the user profile.

Notes:

- The oscomponent.defaultfile.permission parameter defines the baseline for file permissions. The umask value further restricts which permissions are allowed to determine the final file permission. The umask value can be set in the oscomponent.umask parameter, the user profile, the job profile, and other sources.

- For job logs, spool files, and wrapping scripts, the agent determines the final file permission using the oscomponent.defaultfile.permission and oscomponent.umask parameters.

- For standard output and error files, the agent determines the final file permission using the oscomponent.defaultfile.permission parameter and the umask value that takes precedence. For example, if you set the umask value in the user profile and job profile, the umask value in the job profile takes precedence. If the umask value is set to 022 in the user profile and 021 in the job profile, the final umask value is 021.

- If you redirect the output of the command in an argument, these parameters do not apply and the file permission depends on the operating system. For example, if you specify the command as "/usr/bin/echo" and the argument as "TEST >> /tmp/TEST.OUTPUT.COMMAND", the file permission of TEST.OUTPUT.COMMAND is unspecified.

- On CA Workload Automation AE, if you get a 4030 completion code, it means that the agent could not read or write to the temporary wrapper script the agent creates. To resolve the error, verify that the combination of oscomponent.defaultfile.permission and oscomponent.umask parameters give the owner at least read and write permission.

Example: Customize the Permissions of the Agent Working Files on CA Workload Automation ESP Edition

In this example, the following agent parameters are set:

```
oscomponent.umask=113
oscomponent.defaultfile.permission=0664
```

When the agent creates the following files, the permissions are set as indicated in parentheses:

- Job logs (-rw-rw-r--)
- Spool files (-rw-rw-r--)

If no user is specified in the job, the permission of the standard output and error files is -rw-rw-r--. If a user is specified in the job with a default umask of 022, the permission of the standard output and error files is -rw-r--r--.

Example: Customize the Permissions of the Agent Working Files on CA Workload Automation AE

In this example, the following agent parameters are set:

```
oscomponent.umask=066
oscomponent.defaultfile.permission=0600
oscomponent.noforceprofile=true
oscomponent.cmdprefix.force=true
oscomponent.profiles.src.delay=true
oscomponent.profiles.global.override=true
```

The job profile has a umask value of 111.

When the agent creates the following files, the permissions are set as indicated in parentheses:

- Temporary working shell scripts (-rwx--x--x)
- Standard output and standard error files (-rw-------)
- Job logs (-rw-------)
- Spool files (-rw-------)

Configure the Agent for Legacy Remote Agent on UNIX

Note: This procedure applies to CA Workload Automation AE only. The CA Workload Automation AE documentation refers to the Remote Agent (auto_remote) as the legacy agent.

CA Workload Automation Agent for UNIX, Linux, or Windows replaces the Remote Agent that was provided with Unicenter AutoSys JM r4.5 and r11. By default, the agent behaves differently than the legacy agent for sourcing job profiles and global profiles, deleting spool files and job logs, and so on. To configure the agent to behave like the legacy agent, manually add or edit the parameters in the agentparm.txt file.

Follow these steps:

1. Change to the agent installation directory.

2. Enter the following command:

   ```
   ./cybAgent -s
   ```

   The agent stops.

3. Open the agentparm.txt file, and edit or add the following parameters, as follows:

   ```
   oscomponent.environment.variable=agent_install_dir/profiles/WAAE.txt
   oscomponent.environment.variable_manager_instance_name_SCH=agent_install_dir/
   profiles/instance_name.txt
   agent.spool.success.autocleanup=true
   runnerplugin.spool.clean.enable=true
   runnerplugin.spool.expire=7d
   agent.resourcemon.enable=true
   filemon.firstscan.skip=true
   oscomponent.joblog.success.autocleanup=true
   oscomponent.noexitcode=256
   oscomponent.auth.pam.svc=sshd
   oscomponent.cmdprefix.force=true
   oscomponent.initialworkingdirectory=USER
   oscomponent.lookupcommand=true
   oscomponent.noforceprofile=true
   oscomponent.profiles.src.verify=true
   oscomponent.profiles.src.delay=true
   oscomponent.profiles.src.order.global.first=true
   security.cryptkey=cryptkey.txt
   ```

   agent_install_dir

   Specifies the path to the directory where the agent is installed.

instance_name

Specifies the name of the CA Workload Automation AE instance.

4. Save the agentparm.txt file.

5. Enter the following command:

```
./cybAgent -a
```

The agent starts and is configured for legacy remote agent.

Notes:

- The oscomponent.environment.variable parameter is set to the location of the WAAE.txt file. The WAAE.txt file defines the environment settings for jobs that are started on behalf of all managers for all instances of CA Workload Automation AE. For more information about the WAAE.txt file and the environment variables, see the *CA Workload Automation AE Administration Guide* or the *User Guide*.

- The oscomponent.environment.variable_manager_*instance_name*_SCH parameter is set to the location of the *instance_name.*txt file. The *instance_name.*txt file includes the path to the auto.profile file, which is one of the several objects that source the environment for a job. For more information about the auto.profile file and how the environment for a job is sourced, see the *CA Workload Automation AE Administration Guide* or the *User Guide*.

- To run CA Workload Automation AE utilities as jobs, ensure that a CA Workload Automation AE client is installed on the computer where the agent is installed. If you have installed the agent on a computer where no other agents were installed previously, copy the WAAE.txt and *instance_name*.txt files from the computer where an agent is installed to the *agent_install_dir*/profiles directory. Then configure the parameters in the agentparm.txt file.

- When you set the following parameters, the agent executes a temporary shell script without sourcing the user profile:

```
oscomponent.noforceprofile=true
oscomponent.cmdprefix.force=true
```

- When you set the following parameter, the agent drops the sourcing of the profiles into the temporary shell script:

```
oscomponent.profiles.src.delay=true
```

- When you set the following parameter, the agent sources the UNIX global profile first before execution:

```
oscomponent.profiles.src.order.global.first=true
```

- When you set the following parameter, the agent verifies the existence of a job profile before execution:

```
oscomponent.profiles.src.verify=true
```

If the job profile does not exist, the job terminates and returns an error.

Configure the Agent for Legacy Remote Agent on Windows

Note: This procedure applies to CA Workload Automation AE only. The CA Workload Automation AE documentation refers to the Remote Agent (auto_remote) as the legacy agent.

CA Workload Automation Agent for UNIX, Linux, or Windows replaces the Remote Agent that was provided with Unicenter AutoSys JM r4.5 and r11. By default, the agent behaves differently than the legacy agent for sourcing job profiles and global profiles, deleting spool files and job logs, and so on. To configure the agent to behave like the legacy agent, manually add or edit the parameters in the agentparm.txt file.

Follow these steps:

1. Change to the agent installation directory.

2. Stop the CA Workload Automation Agent (*MYAGENT*) service from the Windows Service Control Manager.

   MYAGENT

   Specifies the name of the agent.

3. Open the agentparm.txt file, and edit or add the following parameters, as follows:

   ```
   oscomponent.environment.variable=agent_install_dir\Profiles\WAAE.txt
   oscomponent.environment.variable_manager_instance_name_SCH=agent_install_dir\
   Profiles\instance_name.txt
   agent.spool.success.autocleanup=true
   runnerplugin.spool.clean.enable=true
   runnerplugin.spool.expire=7d
   agent.resourcemon.enable=true
   filemon.firstscan.skip=true
   oscomponent.joblog.success.autocleanup=true
   oscomponent.noexitcode=256
   oscomponent.cmdprefix.force=true
   oscomponent.cmdprefix.force.quotes.full=true
   oscomponent.initialworkingdirectory=USER
   oscomponent.lookupcommand=true
   security.cryptkey=cryptkey.txt
   ```

   agent_install_dir

   Specifies the path to the directory where the agent is installed.

   instance_name

   Specifies the name of the CA Workload Automation AE instance.

4. Save the agentparm.txt file.

5. Start the CA Workload Automation Agent (*MYAGENT*) service from the Windows Service Control Manager.

   The agent starts and is configured for legacy remote agent.

Notes:

■ The oscomponent.environment.variable parameter is set to the location of the WAAE.txt file. The WAAE.txt file defines the environment settings for jobs that are started on behalf of all managers for all instances of CA Workload Automation AE. For more information about the WAAE.txt file and the environment variables, see the *CA Workload Automation AE Administration Guide* or the *User Guide*.

■ The oscomponent.environment.variable_manager_*instance_name*_SCH parameter is set to the location of the *instance_name*.txt file. The *instance_name*.txt file contains a set of environment variables for each CA Workload Automation AE instance. For more information about the environment variables and how the environment for a job is sourced, see the *CA Workload Automation AE User Guide*.

■ To run CA Workload Automation AE utilities as jobs, ensure that a CA Workload Automation AE client is installed on the computer where the agent is installed. If you have installed the agent on a computer where no other agents were installed previously, copy the WAAE.txt and *instance_name*.txt files from the computer where an agent is installed to the *agent_install_dir*/Profiles directory. Then configure the parameters in the agentparm.txt file.

Appendix A: Acknowledgements

This appendix contains copyright and license agreement information from third-party software used in CA Workload Automation.

This section contains the following topics:

HP-UX JRE v1.6

This Product is distributed with HP-UX JRE v1.6. HP has provided additional copyright notices and information that may be applicable to portions of the HP-UX JRE in the THIRDPARTYLICENSEREADME.txt file that accompanies the HP-UX JRE files.

HP-UX JRE v1.7

This Product is distributed with HP-UX JRE v1.7. HP has provided additional copyright notices and information that may be applicable to portions of the HP-UX JRE in the THIRDPARTYLICENSEREADME.txt file that accompanies the HP-UX JRE files.

JRE v.1.7

This Product is distributed with JRE v.1.7. Use of the Commercial Features of the JRE for any commercial or production purpose requires a separate license from Oracle. 'Commercial Features' means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Software documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. Oracle has provided additional copyright notices and information that may be applicable to portions of the JRE in the THIRDPARTYLICENSEREADME.txt file that accompanies the JRE files and at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

Jython v.2.5.3

This product includes Jython 2.5.3 which is distributed in accordance with the following license agreements:

The Jython License
A. TERMS AND CONDITIONS FOR ACCESSING OR OTHERWISE USING JYTHON
PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the
Individual or Organization ("Licensee") accessing and otherwise using this software
("Jython") in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants
Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze,
test, perform and/or display publicly, prepare derivative works, distribute, and
otherwise use Jython alone or in any derivative version, provided, however, that PSF's
License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2007 Python
Software Foundation; All Rights Reserved" are retained in Jython alone or in any
derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates
Jython or any part thereof, and wants to make the derivative work available to others
as provided herein, then Licensee hereby agrees to include in any such work a brief
summary of the changes made to Jython.

4. PSF is making Jython available to Licensee on an "AS IS" basis. PSF MAKES NO
REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT
LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF
MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF JYTHON WILL
NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF JYTHON FOR ANY INCIDENTAL,
SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR
OTHERWISE USING JYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY
THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its
terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of
agency, partnership, or joint venture between PSF and Licensee. This License Agreement
does not grant permission to use PSF trademarks or trade name in a trademark sense
to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Jython, Licensee agrees to be bound by
the terms and conditions of this License Agreement.

Jython 2.0, 2.1 License
Copyright (c) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 Jython Developers All
rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
Neither the name of the Jython Developers nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS|&"&| AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

JPython 1.1.x Software License.
This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and using JPython version 1.1.x in source or binary form and its associated documentation as provided herein ("Software").

Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a non-exclusive, non-transferable, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright Ã?Â©1996-1999 Corporation for National Research Initiatives; All Rights Reserved" are both retained in the Software, alone or in any derivative version prepared by Licensee.

Alternatively, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the quotes), provided, however, that such text is displayed prominently in the Software alone or in any derivative version prepared by Licensee: "JPython (Version 1.1.x) is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1006. The License may also be obtained from a proxy server on the Web using the following URL: http://hdl.handle.net/1895.22/1006."

In the event Licensee prepares a derivative work that is based on or incorporates the Software or any part thereof, and wants to make the derivative work available to the public as provided herein, then Licensee hereby agrees to indicate in any such work, in a prominently visible way, the nature of the modifications made to CNRI's Software.

Licensee may not use CNRI trademarks or trade name, including JPython or CNRI, in a trademark sense to endorse or promote products or services of Licensee, or any third party. Licensee may use the mark JPython in connection with Licensee's derivative versions that are based on or incorporate the Software, but only in the form "JPython-based _____," or equivalent.

CNRI is making the Software available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

CNRI SHALL NOT BE LIABLE TO LICENSEE OR OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY SO THE ABOVE DISCLAIMER MAY NOT APPLY TO LICENSEE.

This License Agreement may be terminated by CNRI (i) immediately upon written notice from CNRI of any material breach by the Licensee, if the nature of the breach is such that it cannot be promptly remedied; or (ii) sixty (60) days following notice from CNRI to Licensee of a material remediable breach, if Licensee has not remedied such breach within that sixty-day period.

This License Agreement shall be governed by and interpreted in all respects by the law of the State of Virginia, excluding conflict of law provisions. Nothing in this Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee.

By clicking on the "ACCEPT" button where indicated, or by installing, copying or otherwise using the Software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

The command line interpreter is covered by the Apache Software License. See the org/apache/LICENSE file for details.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

 (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

 (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

 (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

 (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

 You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

   5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

   6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

   7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

   8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

   9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

   END OF TERMS AND CONDITIONS

   APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

   Copyright [yyyy] [name of copyright owner]

   Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

 http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

6. This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.