Oracle® Communications ASAP

Release Notes

Release 7.2

E18886-02

November 2013

This document provides release notes for Oracle Communications ASAP release 7.2.

About This Document

This document includes the following sections:

New Features

The new features in this release of ASAP are:

For information about installation, patch, upgrade, and deployment considerations, see *ASAP Installation Guide*.

Extended Platform Support

ASAP introduces support for Oracle Linux to give service providers more flexibility when selecting server platforms. Because the Linux server operating system reduces hardware costs, a Linux-based application also reduces hardware costs. ASAP supports Oracle VM for virtualization. ASAP includes support for Red Hat Enterprise Linux because of the implicit compatibility between Red Hat and Oracle Linux distributions. The complete list of supported server operating systems includes:

- Oracle Linux 5.5+
- Oracle Solaris 10
- IBM AIX 6.1
- Hewlett Packard HP-UX for Itanium 11i

Certification with Oracle WebLogic Server 11gR1

ASAP 7.2.0 is certified with Oracle WebLogic Server 11gR1 (10.3.6). For more information about installation, patches, and configuration, see *ASAP Installation Guide*.

Oracle Communications Design Studio 7.2.2

ASAP is certified with Design Studio 7.2.2. See *Oracle Communications Design Studio Installation and System Administration Guide* for details about installing Design Studio and the ASAP plug-ins. Cartridges from previous versions of Design Studio are compatible with Design Studio 7.2.2 and are automatically upgraded to take advantage of the data modeling enhancements. See "Data Modeling Enhancements Through Data Dictionary Support" for more information.

Data Modeling Enhancements Through Data Dictionary Support

ASAP introduces support for the data dictionary framework within Design Studio. Parameters required for ASAP cartridges are first defined within a dictionary schema and then leveraged as data parameters for specific atomic actions. The dictionary schema may be part of the ASAP cartridge project or a separate model project or it may be part of another Design Studio feature plug-in application (for example, part of an OSM project). Using the data dictionary for ASAP cartridge parameters reduces the complexity of ASAP cartridges and facilitates data sharing across other Design Studio feature plug-in applications.

> **Note:** You must define project dependencies so that Design Studio knows which data elements from different projects are intended for ASAP. See the Design Studio Platform Help for information about managing project dependencies.

ASAP cartridges built using previous versions of Design Studio are automatically upgraded during an activation archive import or when an older activation cartridge project file is opened/imported. For additional information about importing activation cartridge projects see the Oracle Communications Design Studio for Activation Help.

New Activation Routing Model Project

Design Studio automatically creates a new activation routing model project within the Design Studio workspace when one or more activation projects exist. The activation routing model project holds the parameters required for network element routing. See the Design Studio for Activation Help for more information about activation routing model project.

> **Note:** The Activation Routing model project is sealed. You should not unseal it.

Web Service Integration Enhancements

ASAP 7.2 provides an enhanced Web Service API that includes the following features:

- **ASAP data type definitions**: ASAP Web Service API explicitly defines the activation OSS/J data types within the Web Service Definition Language interface.
- **Enhanced transport protocol support**: ASAP Web Service introduces support of HTTP/HTTPS transport protocols and continues to support Java message service (JMS).
- **Additional Web Services operations**: ASAP Web Service adds eleven new operations to better align with the OSS/J API.
- **Security enhancements**: ASAP Web Service introduces access-level security and installation over SSL.

The ASAP distribution also includes a sample Web Service client that sends requests to the ASAP Web Service using JMS. For more information about the ASAP Web Service API see *ASAP Developer's Guide*.

JMS Store and Forward

Oracle recommends the JMS store and forward (SAF) method for integrating Oracle WebLogic service fulfillment applications. Oracle recommends creating an SAF agent and a JMS bridge between the ASAP WebLogic server and the remote application WebLogic server to ensure reliable communication between applications. See *ASAP Server Configuration Guide* for more information.

64-bit JVM Support

ASAP 7.2 introduces support for the 64-bit Java Virtual Machine for the ASAP components that run within WebLogic.

JDBC Multi-Data Source Configuration

ASAP uses WebLogic generic and multi-data sources for communication to an Oracle database configured as an Oracle Real Application Cluster (RAC). Customers who use ASAP with Oracle RAC and are upgrading from a previous release of ASAP must delete the original WebLogic data sources and create new WebLogic data sources. Customers who install ASAP on a single database instance but later decide to migrate to Oracle RAC must also delete the original WebLogic data sources and create new WebLogic data sources. See *ASAP Installation Guide* for information about creating WebLogic generic and multi data sources to an Oracle RAC database.

Documentation Improvements

This release of ASAP introduces a number of documentation enhancements, including three new guides: *ASAP Server Configuration Guide*, *ASAP Security Guide*, and *ASAP Cartridge Development Guide*. These guides are available as part of the documentation media pack on the Oracle software delivery Web site.

Fixes in This Release

This release of ASAP contains all enhancements and bug fixes up to and including release 5.2.4 Patch 13, 7.0.0 Patch 11, 7.0.2 Patch 5, and 7.2.0 Patch 2. Refer to the patch readme files available on the My Oracle Support web site:

https://support.oracle.com/

The following table lists the bugs fixed in this release of ASAP.

Bug No.	Related SR	Description
16615621	3-7017223231	In the OCA Session Manager, stale session entries accumulated in the session list, resulting in the list becoming full, such that OCA users could not log in. Now the data type of the session list is changed so that it is thread-safe, also the session monitoring thread handles exceptions so it does not exit when they are encountered.
16172902	3-6651074231	Option 1 in the asap_security_tool (**Initialize the secure data storage**) was deleting the WebLogic admin user entry even in cases where the user chose 'n' at the **Continue? (y/n)** prompt. This led to problems in logging into OCA because it fails in cases where the WebLogic admin user entry does not exist. Option 1 now deletes the WebLogic admin user entry only in cases where the user chooses 'y' at the **Continue? (y/n)** prompt.
16049772	3-6600381711	An error occurred when logging into the OCA client because of a server-side dependency between an OCA server component and the ASAP Daemon process. While this dependency still exists, the error message is more specific: "Please ensure that the ASAP Daemon is running and try again." This makes the problem easier to diagnose and resolve. You no longer have to restart WebLogic.
15884764	3-6432491931	The 'EXEC_RPC' State Table action was returning the wrong results when called more than once within a work order. The first call returned the correct results, but subsequent calls returned the results from the first call instead of the results from the current call. This problem is now fixed.
15873631	3-6281387071	When an NE primary connect request is sent from SARM's NEP driver thread to an NEP (SARM spawns one NEP_driver thread for each NEP), communication parameters are sent with the request. The parameter labels are populated into the fields of a global static structure variable, which could be overwritten by other NEP driver threads in PRE_EMPTIVE threading mode when 2 connect requests from different NEP driver threads are sent at almost the same time. This could lead to primary connect failures causing work orders to get stuck, if multiple NEPs are used and large number of work orders submitted within a short time. Change the problematic global static variable in SARM's NEP driver to be an instance variable.
14668515	3-6210650161	You could not start the ASAP control server when the database password had expired but there was no warning about the expiry. Before you terminate the ASAP server, a message now indicates that the database password will expire before you try to restart the server.
14529454	N/A	The ASAP security tool prompted for the username, which caused a problem later if you entered credentials other than those of the control database. The ASAP security tool no longer prompts for the username but instead prompts for the control password.

Bug No.	Related SR	Description
14311772	3-5944386021	The SRP_lock_order function may return an incorrect code value, causing the SRP to not send the order to SARM. Modify the SRP_ lock_order function to explicitly set the return code value before returning.
14037043	3-5653215661	The **Resend Completed ASDLs** feature (asap_utils option 11) resulted in the following error: Incorrect Number of Arguments. The problem is now fixed.
14017909	3-5641695441	You could not log into OCA using the external LDAP when VNO was enabled because Security Service failed to get the groups information from the external LDAP provider. The Security Service is now fixed to get the groups information from the external LDAP provider so that you can log in when VNO is enabled. The external LDAP provider can be ordered before or after the Default Identity Asserter. Added debug log messages that are turned off by default.
14009819	N/A	The ASAP Security Tool could not change the security level of Class B data. The ASAP Security Tool can now change the security level of the Class B data. If you are upgrading from 7.2.0 GA, 7.2.0 Patch 1, or 7.0.2 pre-Patch 3 and have un-encrypted Class B data, you must perform the following step after applying 7.2.0 Patch 2, before running the ASAP Security Tool for the first time: - Add the configuration parameter **INITIAL_CLASSB_SECURITY_ LEVEL = 0** to the global section of the ASAP.cfg file, and restart the ASAP servers. This step is NOT necessary for a fresh installation of 7.2.0 Patch 2, upgrade from 7.0.1 or earlier releases to 7.2.0 Patch 2, or upgrade from 7.0.2 Patch 3+ to 7.2.0 Patch 2.
13589862	3-5093931031	There was a problem in the handling of RETRY_DIS in the NEP driver. The NE's auxiliary connection counter was not decremented during the disconnects, which resulted in wrong connection counts and caused unexpected behavior in the ASDL dispatch logic. So ASDLs did not progress on some NEs after drop timeout occurred. The NEP Driver in SARM is now fixed to update the NE auxiliary connection count when RETRY_DIS occurs.
13479999	3-1390248681	ASAP periodically got stuck when processing medium-to-high volumes of concurrent 'REPLACE' orders. The problem is now fixed.
13459411	3-4986811911	Work order processing in SARM can be blocked by long running ASAP utilities (asap_utils) sessions. Some asap_utils options (e.g. option 8) locks SARM's data in memory. Work order processing in SARM is blocked until the locks are released. Examples of long running asap_utils sessions include: - running asap_utils in interactive mode and not quitting "more" - suspending asap_utils by Ctrl-Z The asap_utils script is now fixed to prevent work order processing being blocked by long running asap_utils sessions. - redirect output of asap_utils_exec to a file, wait for asap_utils_exec to complete before displaying the temporary file - prevent the asap_utils_exec from being suspended by ignoring the Ctrl-Z signal The asap_utils script is now modified to not remove the existing UTILITY.diag file, so the asap_utils_exec appends the diag messages to the existing file.

Bug No.	Related SR	Description
13391725	N/A	The following JProcessor methods incorrectly truncate strings with more than 255 Polish characters (UTF-8, multibyte): returnInfoParam(); returnGlobalParam(); returnCSDLParam(); returnRollbackParam(); and setASDLExitType(). Modify the JProcessor such that it calculates the string lengths and truncates the strings correctly, taking into account that there could be multi-byte characters in the strings.
13035719	3-3127566661	The SQL SUBSTR function is used in SARM stored procedures to extract the first 80 characters of the parm_vlu string (max size 255 bytes). The returned substring is assigned to parm_subvlu, a variable length character string whose maximum size is 80 bytes. If UTF-8 characterset is used, some of the characters may be multi-byte long. If the substring returned contains multi-byte characters, the string may be longer than 80 bytes, even though the number of characters is 80 or less. Hence the assignment would overflow the 80 byte buffer and cause the ORA-06502 error. Modify the SARM stored procedures to use the SQL SUBSTRB function instead of the SUBSTR function. The SUBSTRB function calculates lengths terms of bytes, not chars. Therefore SUBSTRB(SSP_srq_parm.parm_vlu, 1, 80) would ensure that the substring is at most 80 bytes and fits the parm_subvlu variable and the column in the TBL_SRQ_PARM table.
12407630	N/A	OCA was not able to handle passwords with certain special characters like '&' and '<'. Attempts to log in with these passwords failed. The problem is now fixed. You can use passwords containing any special character.
12355569	3-2076333321	In rare cases, some Java based servers (such as the JNEP and the Daemon) could not start using start_asap_sys.
10360440	3-2346944031	If a Failed order was resubmitted, the OCA client only showed the last instance, which was typically the **Completed** instance. It did not show the previous **Failed** instances. The OCA client now shows all failed and completed instances.
9239218	3-1238872761	ASAP was not generating a **MAINTNCE** event for blackout periods that were detected by the automatic blackout check. The problem is now fixed. ASAP now generates a **MAINTNCE** event in this case.
9211314	3-1194069377	ASAP returned an error on the command-line during shutdown. It occurred when using components that did not include the ASAP **ENV_ID** value in the name. For example, if ENV_ID was **ENV1**, the problem might be triggered by adding a new NEP called **NEP_A**. The problem is now fixed.
8918569	7772171.992	OCA periodically stopped responding in cases where multiple users were running large queries at the same time. The problem is now fixed.
7339679	7045880.993	Control characters were not being removed correctly from NE responses for Java cartridges. The problem is now fixed.
1434446	N/A	Passwords longer than 11 characters caused installation issues on Linux. The problem is now fixed.

The following table lists the enhancements included in this release of ASAP.

Bug No.	Description
14469780	If you set the parameter RESTART_ASAP_SERVERS to true in Design Studio before deploying a cartridge, you no longer have to run the asap_utils script or restart the network processor.
13544420	The size of the EVAL_EXP column of the TBL_CSDL_ASDL_EVAL table is increased from 255 bytes to 1024 bytes.

Known Problems

This section lists the known issues in this release of ASAP.

Bug No.	Description
13839793	The ASAP installer fails to upgrade ASAP when you enable SSL in the wizard. To work around this problem, do not enable SSL in the wizard during the upgrade. Instead, enable SSL after the upgrade is complete: 1. Using the WebLogic Server console for the ASAP server domain, enable any disabled SSL listen ports for all administration and managed servers. 2. Make note of the SSL port values you assigned in the WebLogic Server console. 3. Open the **ASAP.properties** file for editing and add or modify the following parameters: ■ **wls_ssl_enable**: set to **true**. ■ **wls_keystore_file**: set to the full path to the keystore file. ■ **wls_sslport**: set to the SSL listen port for the managed WebLogic server. ■ **wls_admin_port**: set to the SSL listen port for the administration WebLogic server. 4. Open the **ASAP.cfg** file for editing and add or modify the following parameters: ■ **BEA_WLS_PORT**: set to the SSL listen port for the administration WebLogic server. See *ASAP System Administrator's Guide* for information about editing configuration or properties files or using the WebLogic Server console.

Bug No.	Description

11783843	The OCA installer does not interact with Windows User Accounts Control correctly. This causes the OCA desktop shortcuts to not execute the OCA client.
	
	Open the desktop shortcut properties and manually change the values in the **Target** and **Start in** fields. The **Target** field needs to contain the path to the javaw.exe and the OCAClient lib. The **Start in** field needs to contain the path to the path to the OCAClient lib.
	
	For example, if the javaw.exe exists in **C:\Windows\SysWOW64** and the OCAClient is installed in the default location (**C:\Program Files (x86)\Oracle Communications\ASAP**), you would modify the fields as below:
	
	■ Modify the **Target** field to read:
	
	`C:\Windows\SysWOW64\javaw.exe -ms64m -mx64m -classpath "C:\Program Files (x86)\Oracle Communications\ASAP\OCAClient\lib\ocac.jar" architel.OCA.OCAClient.app.OCAMain`
	
	■ Modify the **Start in** field to read:
	
	`C:\Program Files (x86)\Oracle Communications\ASAP\OCAClient\lib`

10349370	SRT XPath parameters must include the namespace.

Oracle Communications ASAP Release Notes, Release 7.2, Patch 2
E18886-02