

Oracle® Auto Service Request

Security White Paper

E37468-01

February 2013

This document explains the technical aspects of the Oracle Auto Service Request (ASR). ASR automates the Oracle Support process by using fault event telemetry from your qualified Oracle Servers to initiate a Service Request.

The following topics are described:

- [Introduction to Oracle Auto Service Request \(ASR\)](#)
- [Configuration](#)
- [Oracle Server Telemetry](#)
- [Telemetry Data](#)
- [Auto Service Request Infrastructure at Oracle](#)
- [Authentication Infrastructure](#)

Introduction to Oracle Auto Service Request (ASR)

Auto Service Request automates the Support Services process by using fault event telemetry from your qualified Oracle Servers to initiate a service request. The software infrastructure detects faults at your site and forwards the telemetry data to systems at Oracle for analysis and service request generation. Auto Service Request is included with Oracle Premier Support for Systems and Hardware Warranty contracts.

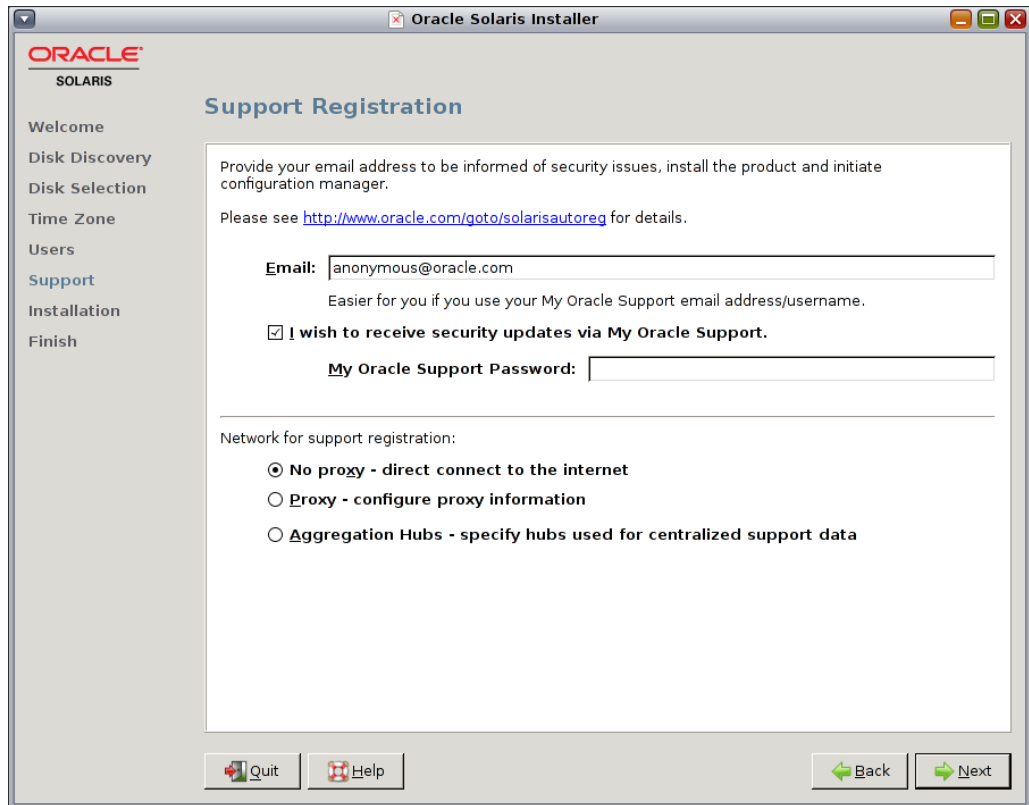
All of the systems that compose the Auto Service Request infrastructure have been built to provide confidentiality, integrity and availability of data. The Auto Service Request security strategy has been designed with multiple layers of encryption, authorization, access controls and data security, to ensure your organizational data is protected.

There are several ASR implementations for various Oracle products. This white paper refers specifically to the ASR client on Oracle Servers. For other ASR implementations, please refer to the specific product documentation.

Configuration

ASR Service can be enabled during the initial Solaris 11 installation. When installing Solaris 11, the following page asks for a valid email address and proxy configuration to send data back to Oracle. Anonymous email address is supported. However, without a valid email address and a service contract, automatic creation of service requests is not enabled.

Figure 1 ASR Configuration



The ASR solution is delivered to the internal product groups through a number of interconnected platforms and systems. These are all built with a focus on security and use defense-in-depth to provide multiple layers of protection.

Oracle Server Telemetry

Once the server is configured to send telemetry via ASR, it sends its configuration, and any faults that occur in XML over HTTPS using the ASR service. On critical faults, a service request is created automatically. This enables Oracle to provide improved support for the server. In order to send data back to Oracle, the server connects to the sites and ports in [Table 1](#).

Table 1 Protocols and Ports

Source	Destination	Protocol	Port	Description
ASR Service	transport.oracle.com	HTTPS	443	Endpoint for sending telemetry messages to the Oracle ASR Service

Telemetry Data

The server collects three types of messages. These include audit messages describing the configuration of the server, fault messages containing description of the faults and a heartbeat message used to determine if the server is up. For details and examples on message types refer to My Oracle Support (MOS) document Sample ASR Messages from Solaris11 (Doc ID 1525772.1):

<https://support.oracle.com/rs?type=doc&id=1525772.1>

All messages sent back to Oracle contain the following information in the header:

- System-id: System serial number.
- Host-id: hostname of the system sending the message.
- Message-time: time the message was generated.
- Product-name: Model name of the server.

Audit Messages

Audit messages are XML messages containing a message header and configuration data. Each message describes the hardware and software components of the server. The hardware components of the telemetry describe model, serial number, and manufacturer for each part. These parts include, CPU, memory, disks etc. The software component contains a list of software packages installed on the server. Once ASR is enabled during install time, the following command can be run to see the data that will be captured and sent to Oracle. The "-n" option prints the data to stdout and does not send it to Oracle.

```
/usr/local/bin/asradm send -n audit
```

Fault Messages

A message (XML) containing the fault description is sent back to Oracle when a hardware fault occurs on the appliance. Each message contains the message header along with the name of the fault, description and other attributes as listed below:

- message-id: is the fault code reported by the fault manager (fmd).
- event-uuid: is the unique identifier for the problem
- event-time: is the time the fault occurred.
- severity: is the severity of the error
- description: is a brief description of the actual error.
- component: has the name of the component where the error occurred.
- summary: a short summary of the event.
- fmdump details: diagnostic details on the component that caused failure from the fault manager (fmd).

To see the fault message contents without sending the data to Oracle, run:

```
/usr/local/bin/asradm send -n
```

Heartbeat Messages

A heartbeat message containing a message header is sent on a daily basis to indicate the server is still alive. The heart message only has a timestamp besides the information in the message header.

Auto Service Request Infrastructure at Oracle

At the heart of the Auto Service Request solution lies the core backend infrastructure hosted within oracle.com. The core ASR infrastructure utilizes user account credentials for validation of users, and digitally signed and encrypted traffic for validation of systems. All of the systems within the Auto Service Request infrastructure require real-time access to the core infrastructure to process alarm and telemetry messages received from end-devices, and to perform authentication lookups.

The core backend infrastructure is a mixture of systems, user interfaces, databases, and web services that are managed and maintained by Oracle. All data stored by ASR is segregated by organization in a multi-tenancy security model, and this security is enforced through multiple layers of API-based access and authorization controls. Data stored within the core infrastructure includes telemetry event data, registration data, ASR asset activation data (including host names and serial numbers, and service requests data).

There is no direct, outside access to the data stores of the Auto Service Request system. All access requests are validated in real-time against the ASR authentication system and pass through multiple layers of security and validation, before being granted access to data elements (for more information, see the next section, Authentication Infrastructure).

Authentication Infrastructure

All requests to the Auto Service Request infrastructure, whether system-generated or human-generated, must pass through multiple layers of business logic and authentication checks in order to gain access to telemetry data.

After passing through perimeter network security measures, requests are first analyzed for proper adherence to system API calls. Requests that use an improper syntax, improperly formatted requests, or requests with a payload that violates prescribed boundaries are immediately discarded at the outermost layer.

If the incoming request is an approved format, the authentication credentials provided with the request are immediately verified against the Oracle Single Sign On (SSO) database for validation. If the credentials presented are authenticated successfully, the request is then compared against the authorization models currently within the system to make sure that the user or system (although authenticated in their identity) has the appropriate level of authorization to perform the request that has been submitted.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Oracle Auto Service Request Security White Paper, Release 4.1
E37468-01

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

This product includes software developed by the JDOM Project.

