# Oracle® Auto Service Request for Sun ZFS Storage Appliances

Security White Paper

**E37468-02**

April 2014

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

The following topics are described:

## Introduction to Oracle Auto Service Request (ASR)

Auto Service Request automates the Support Services process by using fault event telemetry from your qualified ZFS Storage Appliance to initiate a service request. This service 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.

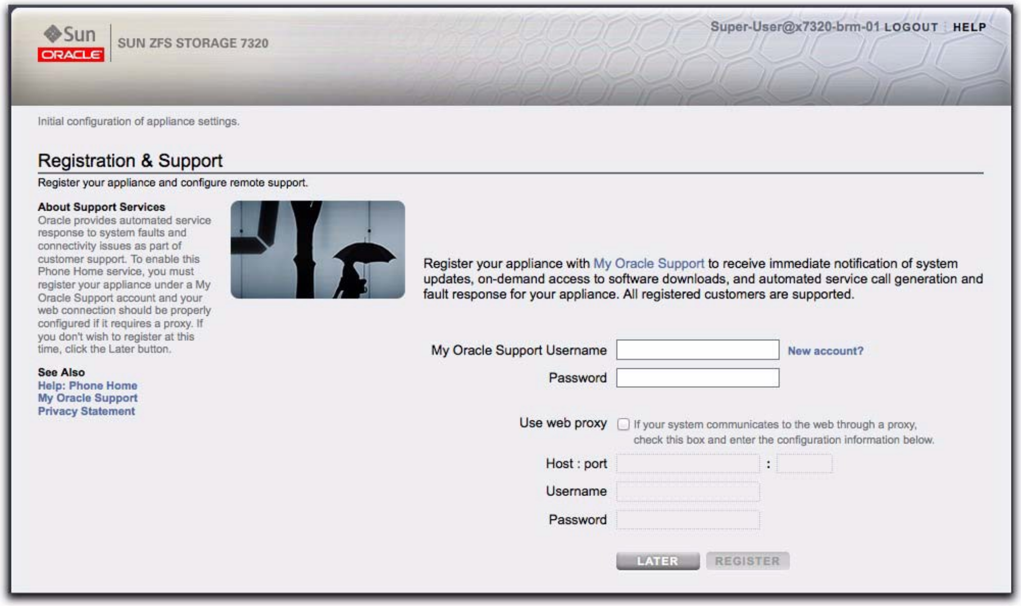
All of the systems that compose the Auto Service Request infrastructure have been built to provide confidentiality, integrity, and availability of data. The Auto Service Request security strategy has been designed with multiple layers of encryption, authorization, access controls and data security, to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

There are several ASR implementations for various Oracle products. This white paper refers specifically to the configuration of ASR for Sun ZFS Storage Appliances. For other ASR implementations, please refer to the specific product documentation.

## Configuration

ASR is enabled within the product during the initial guided setup or later by going to the Configuration>Services>Phone Home Page (Figure 1). The page asks the user for their My Oracle Support username and password in addition to the optional HTTPS proxy information.

***Figure 1 ASR Configuation***



Initial configuration of appliance settings.

Registration & Support

Register your appliance and configure remote support.

**About Support Services**
Oracle provides automated service response to system faults and connectivity issues as part of customer support. To enable this Phone Home service, you must register your appliance under a My Oracle Support account and your web connection should be properly configured if it requires a proxy. If you don't wish to register at this time, click the Later button.

**See Also**
Help: Phone Home
My Oracle Support
Privacy Statement

Register your appliance with My Oracle Support to receive immediate notification of system updates, on-demand access to software downloads, and automated service call generation and fault response for your appliance. All registered customers are supported.

My Oracle Support Username ______ New account?
Password ______

Use web proxy □ If your system communicates to the web through a proxy, check this box and enter the configuration information below.
Host : port ______ : ______
Username ______
Password ______

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.

## ZFS Storage Appliance Telemetry

Once the ZFS Storage Appliance is configured to Phone Home via ASR, the storage appliance sends its configuration, heartbeat 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 better support for the appliance. In order to send data back to Oracle, the appliance connects to the sites and ports in Table 1.

***Table 1 Protocols and Ports***

| Source | Destination | Protocol | Port | Description |
|---|---|---|---|---|
| ASR Service | asr-services.oracle.com | HTTPS | 443 | For sending telemetry messages to ASR Backend. |
| ASR Service | inv-cs.oracle.com | HTTPS | 443 | For sending product registration. |
| Support Bundles | transport.oracle.com<br>(2011.1.9 and later)<br>(2013.1.1.6 and later) | HTTPS | 443 | For sending support bundles that contain state of the appliance during a failure. |

# Telemetry Data

The ZFS Storage Appliance collects three different types of messages. These include audit messages describing the configuration of the appliance, fault messages containing description of the faults and a heartbeat message used to determine if the appliance is up. For details and examples on message types refer to My Oracle Support (MOS) document Sample ASR/Phone Home Messages from the ZFS Storage Appliance (Doc ID 1510567.1), which is a sample telemetry message from the ZFS Storage Appliance:

https://support.oracle.com/rs?type=doc&id=1510567.1

## Message Header

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

- System-id: A unique identifier to indicate serial number of the system.
- Host-id: hostname of the system sending the message.
- Message-time: time the message was generated.
- Product-name: Model name of the ZFS appliance.

## Audit Messages

- Audit messages are XML formatted messages containing a message header and configuration data
- Audit messages are sent once per week or when significant system changes occur.
- Each message describes the following hardware and software components of the appliance.

### Hardware-components

The configuration data from the appliance consists of a list of hardware components. Each hardware component describes the parts of the appliance, such as, disks attached to the appliance, memory and CPU. For each component, following attributes are collected:

- FRU: This stands for field replacement unit that can be replaced to fix a fault that occurs on the appliance.
- Model: is the hardware model.
- Manufacturer: is the hardware manufacturer.
- Serial: is the serial number of the hardware component.
- Revision: is the firmware revision of the component, if applicable.
- Size: memory and disk size, if applicable.

### Software-components

The software components is a listing of the key software installed on the appliance. In order to provide better support, data such as os-version and a list of services on the appliance is collected.

### 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.
- fmdump details: diagnostic details on the component that caused failure from the fault manager (fmd).

### Heartbeat Messages

A heartbeat message containing message header is sent on a daily basis to confirm the ability to phone home when failure conditions occur as well as to indicate when an appliance may not be operating properly.  The heartbeat message only contains the standard header and current timestamp.

### Support Bundles

When a failure is detected, a full system support bundle will be sent to the support files endpoint defined in Table 1. This file will contain system configuration information, log files, and state information, which can possibly include core dumps from the controller. This information is used solely for the purpose of addressing the detected fault and is retained only for seven days after the closure of the associated Service Request.

## 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, hardware and software configuration, and ASR activation 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 initial registration 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.  Following the initial registration with ASR, a private key is generated by the ASR back end service and used by the client for the authentication of all future messages.

## 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](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)

Oracle Auto Service Request Security White Paper, Release 4.1
E37468-02