

Oracle® Auto Service Request
Installation and Operations Guide
Release 3.5 for Oracle Linux and Solaris
E18475-06

November 2011

Copyright © 2011, 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 RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software 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.

Copyright © 2000-2004 Jason Hunter & Brett McLaughlin. 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 disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact.

Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED 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 JDOM AUTHORS OR THE PROJECT 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.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter and Brett McLaughlin. For more information on the JDOM Project, please see <http://www.jdom.org>.

Contents

Preface	vii
Audience	vii
Documentation Accessibility	vii
Conventions	viii
What's New	ix
New Features and Enhancements for Oracle ASR Release 3.5	ix
1 Auto Service Request Overview	
1.1 Auto Service Request Feature Summary	1-1
1.2 ASR Architectural Summary	1-2
1.2.1 Close-Up of the ASR Manager	1-3
1.3 ASR Installation Overview	1-4
1.3.1 ASR Installation Guidelines	1-4
1.3.2 General Installation Considerations	1-4
1.3.3 ASR Installation Milestones Summary	1-5
1.3.3.1 Milestone 1: Designate and Validate ASR Systems	1-5
1.3.3.2 Milestone 2: Assess ASR Systems	1-5
1.3.3.3 Milestone 3: Install the ASR Manager	1-5
1.3.3.4 Milestone 4: Install and Configure ASR Assets	1-6
1.4 Designate ASR Systems	1-6
1.4.1 Designate an ASR Manager System	1-6
1.4.2 Designate ASR Asset System(s)	1-7
1.5 Oracle Auto Service Request Configuration Requirements	1-7
1.5.1 ASR Asset Hardware Requirements	1-8
1.5.2 Operating System Requirements	1-8
1.5.2.1 Oracle Linux (ASR Manager Only)	1-8
1.5.2.2 Solaris	1-8
1.5.2.3 Java Requirements	1-9
1.5.2.4 ASR Manager Network Connection Requirements	1-9
1.5.2.5 ASR Asset Network Connection Requirements	1-9
1.6 Telemetry Sources: Overview and Check	1-10
1.6.1 Confirm Existing Telemetry Sources	1-10
1.6.2 Initially Set-Up and Configure Telemetry Sources	1-11
1.6.3 ILOM General Procedures	1-11

1.6.3.1	ILOM Sideband Management Set-Up	1-12
1.6.3.2	Set Up the Oracle Server Hardware Management Pack (OHMP)	1-13

2 Validate ASR Systems in My Oracle Support

2.1	Request Support Identifier Access in My Oracle Support	2-1
2.2	Review Assets in My Oracle Support	2-2
2.2.1	Access ASR Assets With My Oracle Support Message Center	2-3
2.3	Enable ASR Assets in My Oracle Support.....	2-3
2.4	Oracle Partner Network (OPN) Partners and ASR.....	2-6

3 Install the ASR Manager

3.1	Prerequisite Tasks	3-1
3.2	Install Service Tags	3-2
3.2.1	Install Service Tools Bundle (STB) for Solaris.....	3-2
3.2.2	Install Service Tags for Oracle Linux	3-4
3.3	Check for OASM Installation and Version.....	3-4
3.4	Download the OASM and ASR Packages	3-5
3.5	Install the OASM Package	3-5
3.6	Install the ASR Package	3-6
3.7	Register the ASR Manager.....	3-6
3.8	Enable the HTTP Receiver for Solaris 11 ASR Assets.....	3-7
3.9	Set Up Crontab	3-9

4 Configure and Manage ASR Assets

4.1	Install Service Tools Bundle (STB).....	4-1
4.2	Obtain the ASR Asset Bundle for non-ILOM Telemetry Sources.....	4-1
4.3	Set Up Telemetry Sources to ASR.....	4-2
4.3.1	Enable FMA Telemetry for Solaris 10 ASR Assets.....	4-2
4.3.1.1	Command Line Options for Setting Solaris FMA Trap Destinations	4-3
4.3.2	Enable FMA Telemetry for Solaris 11 ASR Assets.....	4-4
4.3.3	Enable ILOM Telemetry	4-4
4.3.3.1	Enable ILOM: GUI Interface	4-4
4.3.3.2	Enable ILOM: Command Line Interface	4-5
4.3.4	Enable M-Series XSCF Telemetry	4-6
4.4	Activate ASR Assets	4-7
4.4.1	Activate Blade Assets	4-9
4.4.1.1	New ASR Activation on Blade Systems and Chassis.....	4-9
4.4.1.2	Previously ASR-Activated Blade Systems	4-10
4.4.1.3	Sun Blade X6275 Configuration.....	4-11
4.4.2	Activate Exadata Assets.....	4-11
4.4.3	Activate Exalogic Assets	4-12
4.4.4	Activate and Register ASR Assets for Solaris 11 Systems	4-12

5 ASR Environment Administration

5.1	ASR Asset Management.....	5-1
5.1.1	View Status of ASR Asset(s) from the ASR Manager.....	5-2

5.1.2	Review Status of ASR Assets	5-2
5.1.3	Create Test Alert	5-2
5.1.4	Enable/Disable ASR Assets	5-3
5.1.4.1	Disable ASR Assets.....	5-3
5.1.4.2	Enable ASR Assets.....	5-4
5.1.5	Deactivate/Activate ASR Assets.....	5-4
5.1.5.1	Deactivate/Activate ASR Assets from My Oracle Support	5-4
5.1.5.2	Deactivate/Activate ASR Assets from the ASR Manager	5-5
5.1.6	Add/Remove Telemetry Traps from ASR Asset(s).....	5-5
5.1.6.1	Add/Remove Telemetry Traps from Solaris 10 FMA Systems	5-6
5.1.6.2	Add/Remove Telemetry from Solaris 11 FMA Systems	5-7
5.1.6.3	Add/Remove Telemetry Traps from ILOM Systems	5-7
5.1.6.4	Add/Remove Telemetry Traps from M-Series Systems (XSCF)	5-7
5.2	ASR Environment Management.....	5-8
5.2.1	Unregister ASR.....	5-8
5.2.2	Starting and Stopping ASR and OASM.....	5-8
5.2.2.1	Stopping ASR and OASM	5-8
5.2.2.2	Starting ASR and OASM	5-9
5.3	ASR Emails.....	5-9
5.4	ASR Backup and Restore	5-10
5.5	ASR Network Parameters Management	5-11
5.5.1	ASR Port Usage	5-12
5.5.2	Changing the Default SNMP Port for ASR.....	5-12
5.5.3	Configure ASR to Send HTTPS Traffic Through a Proxy Server	5-12
5.5.4	Configure OASM Network Settings	5-13
5.5.5	Test Connectivity from the ASR Manager to Oracle	5-13
5.6	ASR Integration with Enterprise Monitoring Systems.....	5-13
5.6.1	Configuring Trap Files.....	5-14
5.6.2	MIB Location and Data Elements.....	5-15
5.7	Uninstall ASR	5-16
5.8	Upgrade ASR.....	5-17

6 ASR General Troubleshooting

6.1	ASR Diagnostic Utility	6-1
6.1.1	Utility Contents.....	6-1
6.1.2	Delivery Model	6-1
6.1.3	Configure the ASR Diagnostic Utility	6-2
6.2	Service Tools Bundle (STB) Troubleshooting	6-2
6.2.1	Check the STB Agent.....	6-2
6.2.2	Check the Service Tags Version.....	6-3
6.2.3	Check Service Tags Probe.....	6-3
6.2.4	Check Service Tags Listener.....	6-3
6.2.5	Unable to Contact Service Tags on Asset.....	6-3
6.2.6	Service Tags on Asset Reports Unknown or Empty Serial Number/Product Name	6-4
6.2.7	Activation Failed for Asset <asset name> Due to Data Error	6-5
6.2.8	Cannot Retrieve the OASM IP Address	6-5
6.2.9	Services are Disabled: stdiscover or stlisten	6-6

6.3	Check the State of the SMA Service	6-6
6.4	Check the State of ASR Bundles	6-7
6.5	ASR Log Files.....	6-7
6.5.1	Set Log Level	6-8
6.5.2	Set Log File Counts.....	6-8
6.6	Installing ASR Manager on Blade Systems	6-8
6.7	Installing ASR Manager on a Local Zone.....	6-8
6.8	Miscellaneous Errors and Resolution	6-8
6.8.1	Error Messages and Resolutions	6-9
6.8.2	Only One Client Can Access Console at a Time	6-10
6.9	ASR Fault Rules Updates.....	6-10
6.10	ASR Manager Crashed, Move Assets to a New ASR Manager.....	6-11
6.11	ASR - No Heartbeat	6-11
6.12	ASR Assets for Solaris 11	6-12

A ASR E-mail Examples

A.1	ASR Activation E-mail Examples	A-1
A.1.1	Activation Pending My Oracle Support.....	A-1
A.1.2	Activation Failed.....	A-2
A.1.3	Activation Status Change	A-2
A.1.4	Activation Bad Serial.....	A-3
A.1.5	Activation Denied.....	A-3
A.1.6	Status Report	A-3
A.2	ASR Service Request E-mail	A-4
A.2.1	Test Create Success Example	A-4
A.2.2	Test Create Fail Example	A-4
A.2.3	Service Request Create Success Example	A-4
A.2.4	Service Request Create Failed Example	A-5
A.2.5	Partner Service Request Create Example	A-5
A.2.6	Service Request Create is Delayed Example.....	A-6
A.2.7	Draft Service Request Example (non-Partner).....	A-6
A.3	Heartbeat Failure Notification E-mail Examples	A-7
A.3.1	Heartbeat Failure - CAM.....	A-7
A.3.2	Heartbeat Failure - Sun Unified Storage 7xxx	A-7
A.3.3	Heartbeat Failure - ASR SO.....	A-8
A.4	Fault Rules Out of Date E-mail	A-8

Preface

Oracle Auto Service Request (ASR) is a feature of Oracle Premier Support for Systems and Oracle/Sun Limited Warranty that is designed to automatically request Oracle service when specific hardware faults occur. ASR is designed to enable faster problem resolution by eliminating the need to initiate contact with Oracle services for hardware failures, reducing both the number of phone calls needed and overall phone time required. For complete information about ASR, see <http://oracle.com/asr>.

Audience

This document is intended for Oracle customers and partners who have Oracle products qualified for ASR with Oracle Premier Support for Systems and/or Hardware Warranty service plans.

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.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New

Oracle Auto Service Request (ASR) is designed to automatically request Oracle service when specific hardware faults occur. This chapter identifies the features and enhancements provided by Oracle Auto Service Request release 3.5.

The Oracle ASR Manager 3.5 software upgrade is quick to install and is available for download from <http://oracle.com/asr>. All customers are urged to upgrade to this release at their earliest convenience.

Note: Support for Oracle Auto Service Request is limited to the current release and the two previous releases. Oracle now supports ASR 3.3, 3.4, and 3.5. It is recommended that you upgrade to the latest version. See "[Upgrade ASR](#)" on page 5-17 for more information.

New Features and Enhancements for Oracle ASR Release 3.5

The Oracle Auto Service Request Release 3.5 includes the following enhancement:

- Support for devices running Solaris 11. ASR-supported Solaris 11 devices can be found at:

<http://www.oracle.com/technetwork/server-storage/asr/documentation/>

This guide has been updated with instructions and details for configuring ASR for devices running Solaris 11.

Auto Service Request Overview

Welcome to the Auto Service Request (ASR) software from Oracle. ASR is a secure, scalable, customer-installable software feature of Oracle Premier Support for Systems and Oracle/Sun Limited Warranty support that provides auto-case generation when specific hardware faults occur. ASR is designed to enable faster problem resolution by eliminating the need to initiate contact with Oracle for hardware failures, reducing both the number of phone calls needed and overall phone time required. ASR also simplifies support operations by utilizing electronic diagnostic data. If your qualified system is under warranty or covered by a service plan, you are entitled to ASR at no charge. Visit the Oracle ASR product page (<http://www.oracle.com/asr>) for information to see which server, storage, and Oracle Exadata products are qualified for ASR.

Note: ASR is not a monitoring solution and is not a substitute for the normal monitoring processes/services that customers have.

This document provides complete instructions to install the ASR software. Before beginning the installation, review the following topics in this section:

1.1 Auto Service Request Feature Summary

ASR provides the following features:

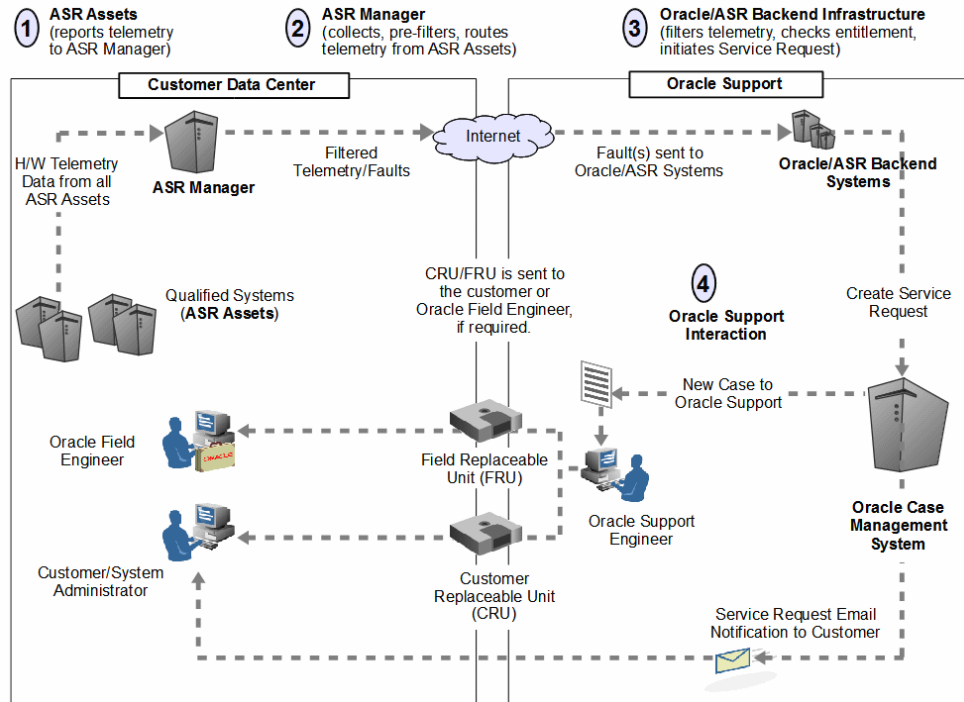
Telemetry Collection and Forwarding: ASR collects specific hardware telemetry data from all ASR-enabled systems, called ASR Assets. ASR filters this telemetry data and forwards what it determines to be potential hardware faults directly to Oracle. Hardware faults cover faults coming from fans, to power supplies, disks, memory, CPUs, and other internal hardware components. The fault telemetry sent to Oracle includes specific hardware faults, but also includes the conditions that may later result in a component failure. The ASR fault coverage is different for each qualified system type.

Automatic Creation of Service Requests: Once fault telemetry is sent to Oracle's ASR infrastructure, systems filter the data again to confirm the reality of the fault and then automatically generates a Service Request. Once created, Service Requests are sent to Oracle Support and also communicated, via e-mail, to the technical support contact on record for the qualified system reporting the fault.

Support Response: Service Requests are actively reviewed by Oracle Support Services and service response is provided in accordance with your Service or Warranty contract.

1.2 ASR Architectural Summary

Whether this is a new installation of ASR, or if you already have some familiarity with the ASR software, it is highly recommended that you review the ASR architecture discussed below. Understanding the architecture and the nomenclature of ASR is key to a successful installation. The following diagram shows the end-state environment once ASR is installed. Use the numbered indicators in the diagram to review it in sequential order and for corresponding explanations in the text that follows.

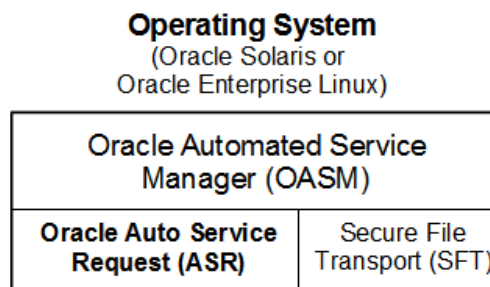


- ASR Assets:** ASR Assets are qualified systems that are configured to report its hardware telemetry to an ASR Manager.
- ASR Manager:** The ASR Manager is a system that centrally accepts hardware telemetry data sent from a group of ASR Assets. The ASR Manager filters the incoming data and forwards potential fault telemetry to Oracle/ASR Backend systems. Additional features of the ASR Manager include the following:
 - The ASR Manager is always installed first, followed by ASR Assets.
 - You have the option to install more than one instance of an ASR Manager. The reasons to do this may be to support a large amount of ASR Assets and/or for organizational reasons, such as grouping ASR Assets by data center, support group, subnet, or other grouping scheme as desired by the customer. An ASR Asset communicates its telemetry to one ASR Manager only.
 - The ASR Manager system can be installed as an ASR Asset. This way, the ASR Manager system can report its hardware telemetry, as does an ASR Asset.
 - The telemetry data that is sent from the ASR Manager to the Oracle /ASR Backend Systems is encrypted. For more information on this topic, refer to the ASR White Paper at: <http://www.oracle.com/asr>.
 - Refer to "Close-Up of the ASR Manager" for more information on the ASR Manager system.

3. **Oracle/ASR Backend Systems:** The ASR backend infrastructure at Oracle collects all telemetry data forwarded to it from the ASR Manager, or ASR Managers if multiple instances are installed. The fault rule technology on these backend systems ascertain the reality of the fault telemetry, and forwards recognized faults to Oracle's Service Request system. From there, the following actions occur:
 - A Service Request, also called a case, is created and assigned to an Oracle Support Engineer. At the same time, an email notification of the Service Request is sent to your support contact on record associated with the system reporting a fault.
 - The Service Request is handled in accordance with the asset's Support or Warranty contract.
4. **Oracle Support Interaction:** Once an Oracle Support Engineer begins working on the Service Request, the engineer may collect additional information from you to better determine resolution to the hardware issue. Resolution to the issue may involve system configuration or the following possibilities:
 - Order and ship a replacement part with installation instructions to you. These are called Customer Replaceable Units (CRUs).
 - Order and ship a replacement part to the customer site to be installed by an Oracle Field Engineer. These are called Field Replaceable Units (FRUs).

1.2.1 Close-Up of the ASR Manager

The ASR Manager software runs as a plug-in application to the Oracle Automated Service Manager (OASM) software. OASM is an applications environment that manages various plug-in applications used mainly for system-level management. OASM simplifies different Oracle Network Service deployments and provides a secure transport mechanism for telemetry data. In addition to ASR, an example of another OASM plug-in application is Secure File Transport (SFT). The diagram below shows the relationship between ASR, OASM, and SFT.



1.3 ASR Installation Overview

This section summarizes the ASR installation process so that customers are better prepared to install ASR.

- Prerequisites overview
 - Valid Oracle Support Contract
 - Access to My Oracle Support
 - Customer Support Identifier
 - Identify ASR Manager and Assets
- Download and install the ASR package
 - Download ASR and Services Tools Bundle (STB) packages
 - Identify Telemetry sources
 - Configure ASR Manager and Assets
 - Register ASR Manager and Assets
- Using ASR
 - ASR e-mails
 - Updating traps
 - Troubleshooting and support

1.3.1 ASR Installation Guidelines

Keep the following guidelines in mind when installing ASR:

- Installing ASR consists of installing an ASR Manager followed by ASR Assets. The ASR Manager system is always installed first. Once the ASR Manager is installed and activated, ASR Assets can be added or removed as needed. For more on the roles of these ASR components, refer to "[ASR Architectural Summary](#)" on page 1-2.
- Installers of ASR should have systems administration experience and some measure of support responsibility for the systems where ASR is to be installed.

1.3.2 General Installation Considerations

The ASR installation process may vary given the differences across computing environments. This document makes every attempt to accommodate these differences, but it is helpful to be aware of the following considerations that may alter the process:

- **Hardware Platform:** Some hardware may not support the installation of ASR. This document provides the platform criteria for ASR installation. Visit the Oracle ASR product page (<http://www.oracle.com/asr>) to see which server, storage, and Oracle Exadata products are qualified for ASR.
- **Operating System Version:** The operating system version – either Oracle Linux or Solaris – may impact the ASR installation. Some platforms may require an operating system update and/or a patch upgrade.
- **Existing Hardware Telemetry Sources:** The existing telemetry sources on systems may impact the installation of ASR. In some cases, telemetry software may need to be upgraded.
- **Access to My Oracle Support:** You must have a login and access to My Oracle Support (<http://support.oracle.com>) before installing ASR.

- **Accuracy of Data in the My Oracle Support Database:** A key task to installing ASR involves validating hardware serial numbers, contract levels, and support contacts in the My Oracle Support database. If this data is inaccurate, you will have to correct it. ASR relies on the accuracy of this data to verify service entitlement, to ensure the proper routing of Service Requests, and to ensure the correct support personnel are contacted when specific systems send fault telemetry.

1.3.3 ASR Installation Milestones Summary

Refer to the following sections for a summary of the major milestone steps with installing Oracle Auto Service Request.

1.3.3.1 Milestone 1: Designate and Validate ASR Systems

This milestone determines which host system will have the ASR Manager installed. It includes sizing the system and ensuring it is qualified for ASR. This milestone also consists of determining which systems will be installed as ASR Assets and ensures that they too are qualified for ASR.

This milestone also involves accessing My Oracle Support and validating/ updating key information in its database. This information includes hardware serial numbers, contract levels, and support contacts.

1. Select systems for ASR implementation (ASR Manager, ASR Assets)
2. Qualify systems for ASR support.
3. Register/access My Oracle Support.
4. Validate system information (active contract, serial number, technical contacts, etc.).

1.3.3.2 Milestone 2: Assess ASR Systems

This milestone involves assessing the state of the systems designated for ASR installation. Items reviewed include an operating system version check, Java (JRE/JDK) version check, a check of proper network connectivity, and to confirm the specific hardware telemetry sources installed on the systems.

Depending on the results of the systems assessment, this milestone may involve installing appropriate OS patches, Java updates, and network configurations.

1. Verify Oracle Linux or Solaris version and patch level.
2. Confirm network setup and connectivity.
3. Confirm Java version (for the ASR Manager system only).
4. Confirm telemetry sources on all ASR systems.
5. Set up telemetry sources (e.g., ILOM).

1.3.3.3 Milestone 3: Install the ASR Manager

This milestone includes installing supporting software that may be required for ASR, depending upon your qualified platform. This may include the Service Tools Bundle (STB), for example.

Once the above milestones are complete, the ASR Manager can be installed. This milestone, along with installing ASR Assets, is the quickest part to the overall installation.

1. Download the latest Oracle Automated Service Manager (OASM) and ASR packages.
2. Install the OASM and ASR packages.
3. Register and validate the ASR Manager.

1.3.3.4 Milestone 4: Install and Configure ASR Assets

The last milestone to installing the ASR environment is to configure ASR Assets and validate the installation. Configuring ASR Assets may involve installing supporting software, such as Service Tools Bundle (STB) or Service Tags.

Note: Service Tags and `asrassetbundle` are not required for Solaris 11.

1. Install Service Tools Bundle (STB) or Service Tags.

Note: STB is required for Solaris 10 ASR Assets and optional for Solaris 11 ASR Assets.

2. Obtain the ASR Asset Bundle (via shell script).
3. Configure ASR telemetry sources to send events to the ASR Manager.
4. Activate ASR Asset(s).
5. Login to My Oracle Support (<http://support.oracle.com>) to complete activation of the asset.
6. Review all ASR Asset status in My Oracle Support.
7. Generate a test alert to validate data transmitted to Oracle (results are emailed to the ASR administrator).
8. Repeat steps for each ASR Asset.

1.4 Designate ASR Systems

This section explains how to initially designate which system will have the ASR Manager installed and which systems will be installed as ASR Assets. This process involves sizing the systems and making sure all the systems are qualified for ASR.

1.4.1 Designate an ASR Manager System

Use the following procedure to designate an ASR Manager system. To use these instructions, it is important to understand the difference between an ASR Manager and an ASR Asset system.

1. Choose a system that you intend to install as the ASR Manager. This system does not need to be a dedicated server and can co-reside with other applications and services. See "[Oracle Auto Service Request Configuration Requirements](#)" on page 1-7 for information about operating system and Java requirements.

Note: The ASR Manager can be installed on a database server in Oracle Database Machine. However, Oracle recommends that it is installed on a standalone server.

2. Size the system:
 - Establish roughly how many ASR Assets will report their hardware telemetry to the ASR Manager system now and in the future
 - Refer to the Hardware and Network Configuration page (see <http://www.oracle.com/asr> for more information) to confirm system requirements, depending on how many ASR Asset(s) will report their telemetry to the ASR Manager.
 - If the system you selected to be an ASR Manager is under-sized, consider the following options:
 - Select another system that is better sized, or upgrade the current system.
 - Reduce the number of ASR Assets that you will associate to this ASR Manager system. If you choose this option, you will have to consider installing an additional instance(s) of the ASR Manager to accommodate the remaining ASR Assets. Focus on the first ASR Manager and its associated ASR Assets before installing additional ASR Manager instances.
3. Once the ASR Manager is sized, record the hostname and hardware type.

1.4.2 Designate ASR Asset System(s)

Follow the procedure below to designate ASR Asset system(s). To use these instructions, it is important to understand the difference between an ASR Manager and ASR Asset systems. Refer to "[ASR Architectural Summary](#)" on page 1-2, if needed.

Note: The ASR Manager system is always installed first. If you have not completed the installation of the ASR Manager, go to "[ASR Installation Overview](#)" on page 1-4.

1. Choose the qualified systems that you intend to install as ASR Assets and make note of the hardware type of each (for example, Sun Fire V490, E12K, SPARC Enterprise T5120, Sun Blade X6240, etc.).
2. Verify your system is qualified for ASR. Visit the Oracle ASR product page (<http://www.oracle.com/asr>) to see which server, storage, and Oracle Exadata products are qualified for ASR.

From the Qualified Systems List, confirm that your system is on the list. If not, the system is not yet qualified to run ASR.
3. Once the ASR Asset system(s) are qualified, record the hostname(s) and hardware type of each. Use your own mechanism for tracking this information or use tracking forms provided in "[ASR E-mail Examples](#)" on page A-1.

1.5 Oracle Auto Service Request Configuration Requirements

This section provides the instructions to assess your Oracle system environment for the ASR installation. An assessment of your operating system version, network setup,

and available telemetry sources is necessary to determine if any of these items need upgrading or other configuration to support the ASR installation.

Note: The instructions in this section apply to both the ASR Manager and ASR Assets.

1.5.1 ASR Asset Hardware Requirements

For ASR Assets, only the hardware listed on the Systems Qualified for ASR page is supported. Visit the Oracle ASR product page (<http://www.oracle.com/asr>) to see which server, storage, and Oracle Exadata products are qualified for ASR.

Qualified ASR Asset hardware must be associated with a valid support identifier in My Oracle Support (<https://support.oracle.com>).

Note: Oracle Auto Service Request Release 3.1 no longer requires the designated ASR Manager to be qualified. However, there are still minimal operating system, Java, telemetry, etc., requirements.

1.5.2 Operating System Requirements

Designated ASR Managers support Oracle Auto Service Request running Oracle Linux or Solaris operating systems.

Note: ASR Assets support Oracle Auto Service Request running Solaris. If you choose to include your ASR Manager as an ASR Asset, it must be running the Oracle Solaris operating system.

1.5.2.1 Oracle Linux (ASR Manager Only)

Two versions of Oracle Linux are supported:

- Oracle Linux 5.3 or later is supported for ASR.
- Oracle Linux 5.5 with Oracle Unbreakable Linux Kernel (version 2.6.32-100.0.19.el5)

To check your systems, run `/etc/enterprise-release`. The output should look like this:

```
Enterprise Linux Enterprise Linux Server release 5.3 (Carthage)
```

1.5.2.2 Solaris

The following Solaris releases are supported for ASR Manager systems:

- Solaris 11
- Solaris 10, Update 6 (10u6), or later

To check your Solaris version, run `cat /etc/release`.

If your qualified ASR Asset indicates a particular patch version, verify your patch level (see <http://www.oracle.com/asr> for information on Solaris requirements for Server Products Qualified for ASR):

```
patchadd -p|grep patch number
```

To download any required patches, visit My Oracle Support (login required) at <http://support.oracle.com>.

1.5.2.3 Java Requirements

ASR Manager (versions 2.5 and higher) systems require at least JDK 1.6.0_04 or later (see JDK 6 on the Java SE Downloads page: <http://java.sun.com/javase/downloads/index.jsp>). This version of Java is required for Oracle Automated Service Manager (OASM) 1.2. To check your version of Java, run:

```
java -version
```

1.5.2.4 ASR Manager Network Connection Requirements

The ASR Manager System must have an internet connection – either a direct connection or through a proxy. If you access the internet through a proxy, check with your network administrator to collect information needed to configure the ASR Manager system. You will need to know:

- Proxy server name
- Proxy port number
- Proxy user name
- Proxy password
- NTLM Domain Name (if applicable)
- NTLM Host Name (if applicable)
- SASM Host Information (if applicable)

Check and make note of the ASR Manager IP address:

```
ifconfig -a
```

To test the connection to Oracle, in a browser, go to:

- <https://transport.oracle.com:443>

You can also test your connection in a terminal window:

- `telnet transport.oracle.com 443`
- `/usr/sfw/bin/wget https://transport.oracle.com`

If you receive a “connected” message, the connectivity is successful.

1.5.2.5 ASR Asset Network Connection Requirements

Contact your network administrator to confirm or enable the following:

1. Set-up firewall rules to allow bi-directional SNMP/UDP traffic to traverse between ASR Assets and the ASR Manager.

Note: If your asset is running Solaris 11, then ensure the designated HTTP(S) port is open to the ASR Manager.

2. Ensure that ASR Assets can send SNMP telemetry data out on port 162 to the ASR Manager.

Note: If your asset is running Solaris 11, then ensure it can send HTTP(S) telemetry data to the ASR Manager port configured.

3. Ensure that the ASR Manager can communicate with ASR Assets, via http, using port 6481.

Note: If your ASR Asset system is running Solaris 11, then this step is not required.

Check and make note of the ASR Asset IP address:

```
ifconfig -a
```

If working with a system that has a service processor, such as Blade systems and some T and X-series systems, obtain the service processor and/or the chassis IP address. These will be required for ASR installation

1.6 Telemetry Sources: Overview and Check

An integral component to ASR functionality is the hardware telemetry sources resident on your ASR Assets. Depending upon your hardware type, you will have one or more hardware telemetry sources resident on your system. Proceed with the installation by continuing to the following sections in order:

- "[Confirm Existing Telemetry Sources](#)". Use this procedure to determine what telemetry sources exist on your hardware.
- "[Initially Set-Up and Configure Telemetry Sources](#)". Based on what telemetry sources exist on your system, some configuration or updates may be required.

1.6.1 Confirm Existing Telemetry Sources

Use this section to determine the existing telemetry sources on your Oracle Sun system. ASR connects to these telemetry sources, collects potential fault data, and forwards it to Oracle for the automatic creation of Service Requests.

1. For ASR Assets, visit the Oracle ASR product page (<http://www.oracle.com/asr>) for list of server, storage, and Oracle Exadata products.
2. Find your hardware platform in the tables.
3. In the columns titled **Telemetry Source on: SERVICE PROCESSOR** and **Telemetry Source on: HOST**, you will see the telemetry sources that are on your system. As indicated, some telemetry sources reside on a service processor (dedicated hardware), and others reside on the host itself. It is also common for some systems to have multiple telemetry sources.
4. Make a note of the telemetry sources on your system for later use in the installation process (for example, ILOM, FMA, XSCF, etc.).
5. If the telemetry sources have a **Note** indicator, review the note at the bottom of the table and make note of the requirements for that telemetry source. Keep the following in mind:

- Any Solaris operating system or patch requirements should have been completed. Refer to "[Operating System Requirements](#)" on page 1-8, if necessary.
- In some cases, the telemetry software must be upgraded for ASR. In other cases, the telemetry source requires a dedicated network connection (for example, ILOM-enabled systems).
- In some cases, multiple telemetry sources cannot run together on the same system. For example, the SPARC Enterprise T5000 series requires that either ILOM or SunMC be used as the telemetry source, not both.

1.6.2 Initially Set-Up and Configure Telemetry Sources

This section defines all possible telemetry sources that could exist on your system. Your specific telemetry sources should already be known, as explained in "[Confirm Existing Telemetry Sources](#)". If you have ILOM telemetry, go to the ILOM section in the list below and follow the specific ILOM instructions. If ILOM is not applicable to you, or you have completed the ILOM instructions, continue to [Chapter 3, "Install the ASR Manager."](#)

1. **Fault Management Architecture (FMA):** FMA is a capability in Solaris 10 and 11 that automatically diagnoses, isolates, and recovers from many hardware and application faults. As a result, business-critical applications and essential system services can continue uninterrupted in the event of software failures, major hardware component failures, and even software misconfiguration problems.
 - Solaris 10 can be configured to send SNMP traps to the ASR Manager.
 - Solaris 11 can be configured to send events to the ASR Manager via http(s) using the Solaris `asradm` command via the `asr-notify` service.
2. **Integrated Lights Out Manager (ILOM):** ILOM is embedded into some platforms and comes with dedicated network and serial ports to provide remote management, configuration, and telemetry reporting. ILOM reports power and environmental problems as well as CPU and memory faults on certain servers.
3. **M-Series Extended System Control Facility (XSCF):** XSCF incorporates a service processor separate from all other processors. XSCF regularly monitors server components including CPU, memory, disks, fan rotation and device temperatures.
4. **The Oracle Hardware Management Pack (OHMP):** OHMP allows ILOM events to be captured by the Host and forwarded through the Host network connection. OHMP is a telemetry source for T5xxx and some x64 servers.
5. **Sun Management Center Agent (SunMC):** SunMC provides power and environmental fault information from the host for some servers and from the system controllers of some high-end servers.

1.6.3 ILOM General Procedures

If you have determined that the ILOM telemetry source is required for ASR, use the following procedure to set-up and/or confirm your ILOM configuration. The instructions provided here are summarized for your convenience. For complete details on configuring ILOM, refer to your ILOM documentation.

1. ILOM requires a network connection/route to the ASR Manager system. If you know that ILOM is already set-up and connected to the network, continue to the next step. Otherwise, continue with the tasks below.

- A network connection must be made from the Net Management port on the system's service processor (SP) to the network.
 - An IP address must be assigned to the Net Management port. Obtain and make note of this IP address for later use in the installation.
 - For some systems, ILOM can be connected using Sideband Management. (See <http://www.oracle.com/asr> for information on systems that use ILOM as a telemetry source.) ILOM Sideband Management allows the same ILOM IP address to be used, but it is routed through one of the host Gigabit Ethernet ports, thus eliminating the need for the physical connection to the ILOM Net Management ports. If you want to configure your ILOM system for Sideband Management, go to "[ILOM Sideband Management Set-Up](#)". When complete, return and continue with the following instructions.
2. Confirm the ILOM version. Refer to the list of qualified servers (see <http://www.oracle.com/asr>) to determine if the version of ILOM running on your platform is supported by ASR.
 - Use `ssh` to the IP address of the ILOM network interface and log in as root.

```
ssh IP_Address_of_ILOM_Interface
```
 - Run the following command:

```
show /SP  
or  
version
```
 3. If the product version is earlier than 2.x, upgrade it now to the latest ILOM version using your ILOM documentation for instructions.
 4. When you have confirmed that ILOM is enabled and properly networked, continue to "[Install the ASR Manager](#)".

1.6.3.1 ILOM Sideband Management Set-Up

ILOM Sideband Management allows ILOM telemetry to be routed through the Host Ethernet port. This shared connection using the Host Ethernet port eliminates the physical connection required for the ILOM Net Management port.

Note: Connection to the SP using `ssh` or the web interface may be lost during configuration of Sideband Management.

The default ILOM network connection is through the Service Processor's dedicated network port.

Note: ILOM Sideband Management is currently available for specific Oracle x64 and Coolthreads servers. Visit the Oracle ASR product page for a complete list of all hardware qualified for ASR:
<http://www.oracle.com/asr>

1. Login to the host and confirm the mac address:

```
# ifconfig -a
```

Output will look similar to this:

```

lo0: flags=2001000849
<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000

e1000g0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 2
    inet 10.10.10.235 netmask fffffe00 broadcast
10.10.10.255
ether 0:3:ba:d8:b4:5c <---- This line shows an example of the mac address.

```

Note: Make sure to set the ILOM port to a connected and configured Host Ethernet port. The mac address obtained from the host is the Ethernet port that should be used.

2. Login to ILOM using the web interface and configure ILOM trap destination to ASR Manager. See "[Enable ILOM: GUI Interface](#)" on page 4-4 or "[Enable ILOM: Command Line Interface](#)" on page 4-5 for details.
3. Configure the ILOM for Sideband Management; select the **Configuration** tab and then the **Network** tab.
4. Select the ILOM Sideband Management Port by using the drop-down list to activate the desired management port. The SP Network Management Port /SYS/SP/NET0 is the default setting, and the drop-down list allows the user to change to any of the four Host Ethernet ports /SYS/MB/NETx, where x is 0 to 3.
5. Click **Save** for the changes to take effect.

1.6.3.2 Set Up the Oracle Server Hardware Management Pack (OHMP)

The Oracle Hardware Management Pack (OHMP) allows ILOM events to be captured by the Host and forwarded through the Host network connection. This eliminates the need to network the Service Processor. The host must be configured and activated for ASR to properly forward ILOM telemetry. The OHMP is only available on certain systems.

Note: The OHMP for ASR is only available for certain systems using Solaris 10. For more information about specific systems visit the Oracle ASR product page (<http://www.oracle.com/asr>).

The host must be activated for ASR and trap destinations configured.

1. Configure the host trap destination to the ASR Manager as described in "[Enable FMA Telemetry for Solaris 10 ASR Assets](#)" on page 4-2.
2. Download and install the latest Oracle Service Hardware Management Pack. To download OHMP:
 - a. Login to My Oracle Support (<https://support.oracle.com>).
 - b. Click the *Patches & Updates* tab.
 - c. In the Patch Search pane, click *Product or Family (Advanced Search)*.
 - d. Enter **Oracle Hardware Management Pack** in the Product field.
 - e. In the Release drop-down menu, select the release of OHMP you want to download and click the *Search* button.

- f. In the Search Results, click the Patch ID number that corresponds to your operating system (the applicable operating system is shown in the Patch description).
 - g. In the patch description, click the *Download* button to download the patch
3. Use the *Oracle Hardware Management Pack Installation Guide* to install OHMP. Please note the reference to CR 6977584 (Unix Installer Issue) in the Installation Issues section of the manual. When using the OHMP installer, if the installation aborts, it is likely to be due to this defect. There are two workarounds for this defect:
- a. Use the command `unsetenv DISPLAY` to unset the `DISPLAY` variable before running the installer. The `unsetenv` command runs in the C shell.
 - b. Install the required components of OHMP manually rather than using the OHMP installer. The procedure for manual component installation is included in the *Oracle Hardware Management Pack Installation Guide*. The packages required to support OHMP telemetry are:

```
ORCLhmp-libs  
ORCLhmp-snmp  
ORCLhmp-hwmgmt
```

4. Activate the host for ASR as described in "[Activate ASR Assets](#)" on page 4-7.

Validate ASR Systems in My Oracle Support

My Oracle Support provides an interface to the ASR service: both for activation of ASR Assets and for viewing any Service Requests generated from ASR.

With your valid, Oracle Premier Support or Warranty contract, you will need to access My Oracle Support to complete the ASR activation process. You can also view all hardware assets associated with your support identifier.

This chapter includes instructions for using My Oracle Support to perform the following tasks:

- Requesting support identifier access
- Viewing Assets
- Enabling ASR Assets

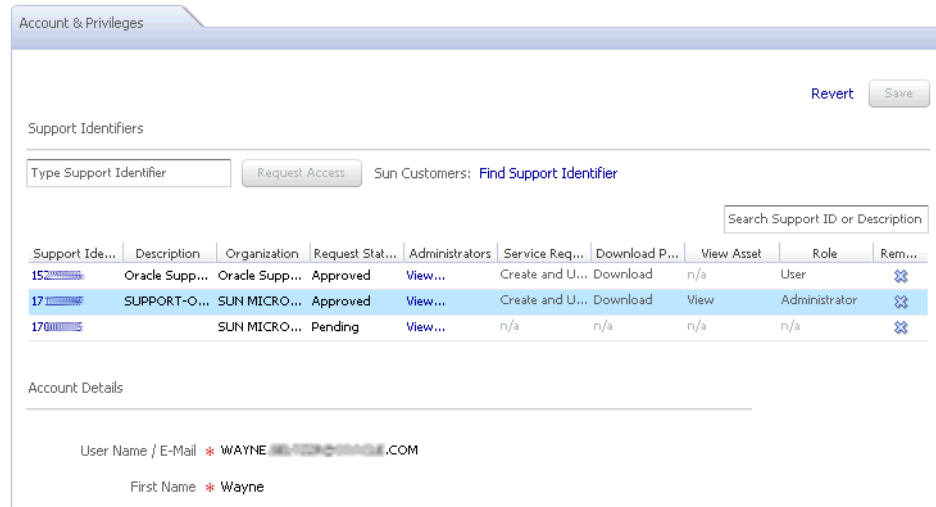
To install the ASR software components, you must provide a valid My Oracle Support login name in order to validate key information about the systems targeted for ASR installation (for example, serial numbers).

2.1 Request Support Identifier Access in My Oracle Support

With Oracle Premier Support, a support contract is composed of one or more support identifiers. Each support identifier can cover one or more hardware assets. You **must** have the appropriate account access before you can complete any ASR installation. Only the Customer User Administrator (CUA) can approve an ASR Asset.

To request access to your support identifier:

- Login to My Oracle Support (<https://support.oracle.com>). Note that your Oracle Single-Sign On user name is your email address. You can register if you are a new user.
- In the My Oracle Support Dashboard, click the “More...” tab. Then select “Settings” from the menu.
- In the “Settings” pane on the left, select “Account & Privileges” (located under the Personal submenu). Information about your account and access privileges will display:



- If you already have the support identifier number, enter it in the field and click the “Request Access” button. If you do not know your support identifier, click “Find Support Identifier” to perform a search. You can search on:
 - The hardware system serial number
 - Organization
 - Existing Sun Contract number
- Access requests are sent to the account administrator to approve. Once approved, you will be able to view information about the assets associated with your support identifier.

2.2 Review Assets in My Oracle Support

Once you have access to your appropriate support identifier, you can review all hardware assets associated with it. To view all assets associated with your support identifier:

- Login to My Oracle Support (<https://support.oracle.com>).
- In the My Oracle Support Dashboard, click the “More...” tab. Then select “Settings” from the menu.
- In the “Settings” pane on the left of the window, select “Assets” (located under the Administrative submenu). All assets associated with your support identifier will display.
- The last column of the table shows the asset's “ASR Status.” There can be four values for this field:
 - **Active:** ASR is active for this asset.
 - **Inactive:** the asset has the correct ASR software installed, but it is not active. Assets can be set to “inactive” for any number of reasons (e.g., asset maintenance, patch updates, contract expiration).
 - **Pending:** the asset has the correct ASR software installed, but has not yet been enabled. See the next section (“[Enable ASR Assets in My Oracle Support](#)”).
 - **[Empty]:** The asset has not sent an ASR activation request to Oracle.

You can view information about a particular asset, and in some cases, you can update information about the asset. To view the information, click the asset's serial number. You can update the following content:

- **Asset Name:** you can give the asset an alias to help system administrators readily identify a particular system. This option can be useful if there are many qualified assets associated with the support identifier or if you want to specifically call out an ASR Master system.
- **Contact Name:** the name of the person responsible for the particular machine. This name should be either a system administrator, primary developer, etc. All assets configured for ASR must have a contact name. An asset cannot be enabled without this information. The Contact's Customer Support Identifier must be approved in My Oracle Support in order for the Contact to view assets.
- **Address:** the address fields should indicate the location of the asset.

Note: For more information on how to use My Oracle Support, click the Help link in the upper-right-hand corner.

2.2.1 Access ASR Assets With My Oracle Support Message Center

My Oracle Support includes a Message Center to show when a user action is required. If you have the correct association to a support identifier, then you will receive a message when the following ASR actions are required:

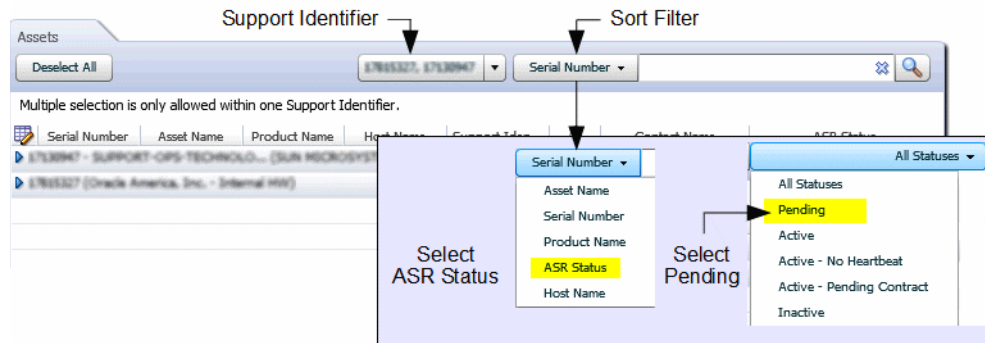
- Show Assets with ASR 'No Heartbeat' Issue
This message indicates a network or connection problem with the ASR Asset.
- Approve ASR Assets
As new qualified hardware is associated with a support identifier, they need to be approved to be ASR Assets. This message shows when an ASR Asset is awaiting approval. The ASR service will not be enabled for the asset until it is approved in My Oracle Support.

2.3 Enable ASR Assets in My Oracle Support

To complete the installation of ASR, you will need to login to My Oracle Support. To complete the installation of ASR:

1. Install the ASR software:
 - See "[Install the ASR Manager](#)" on page 3-1 for instructions to install the ASR Manager software.
 - See "[Configure and Manage ASR Assets](#)" on page 4-1 for instructions to install ASR software on qualified assets.
2. Activate the ASR Asset from the ASR Manager. This step will allow the asset to be approved or denied for ASR activation with My Oracle Support:
 - Register and verify the ASR Manager (see "[Register the ASR Manager](#)" on page 3-6)
 - Activate for ASR Assets (see "[Activate ASR Assets](#)" on page 4-7)
3. Login to My Oracle Support (<https://support.oracle.com>).
4. In the My Oracle Support Dashboard, click the "More..." tab. Then select "Settings" from the menu.

5. In the "Settings" pane on the left of the window, select "Assets" (located under the Administrative submenu). For your Support Identifier, select "ASR Status" from the sort filter, then select Pending from the "All Statuses" drop-down menu:



Note: By default, all support identifiers that you are associated with are displayed. If this list of assets is long, you can limit the display to show only assets associated to one support identifier.

You can filter and sort on asset columns to find the assets you are interested in.

6. You can approve a Pending asset two ways:

- Activate via Asset Toolbar

Click the asset's serial number to display a toolbar with following options:

- Assign Contact - select this option to assign a contact to the asset. Only users associated with the support identifier can be a contact.
- Change Address - select this option to update the asset's physical location.
- Approve - for assets that are Pending, click Approve to enable ASR for the asset.
- Other Actions - you can also perform other actions such as Activate (for an inactive asset), Deactivate (for an active asset), or Deny (for a pending request).

The Asset Toolbar looks like this:



Note: You can use the Asset Toolbar to update multiple assets. To select multiple assets:

1. Click the checkbox of each asset.
2. Click the first asset then shift-click another asset to select all the assets in a range.

- Activate via Asset Details

At the bottom of the Asset pane, there is a "Show Asset Details" option. Click an asset's serial number and then the "Show Asset Details" to update information about the asset. The ASR Activation window will appear and look like this:

Required fields for ASR asset activation are indicated by an asterisk (*). You should update and verify the following fields:

- **Asset Name:** You can assign a name for the asset.
- **ASR Status:** This field shows the current status of the ASR Asset. For Pending assets, click the Approve button to enable the asset for ASR.

Note: There can be many reasons to deny ASR activation. For example, if the machine is part of a test environment and you do not want to receive status email from ASR, then you can click the Deny button to exclude it from ASR. You can always update the settings for the machine to include it.

- **Contact Name:** Users that have been associated with the Support Identifier for the asset will appear in this drop-down menu. Click the drop-down menu to see the list of available names.
- **Street Address 1:** Enter the street address for the physical location of the asset.
- **Country:** Select the asset's country location from the drop-down menu.
- **ZIP/Postal Code:** enter the ZIP/postal code for the asset's location.
- **Distribution Email List:** You may add an email address that will receive all ASR email notifications (for example "asr_notify@mycompany.com"). Oracle ASR will send email to the Contact's email address **and** the Distribution Email List, if provided. You may also include multiple email addresses, separated by commas (for example, "asr_notifyteam1@mycompany.com, asr_notify_team2@mycompany.com"). This feature is useful if your organization has one or more teams that should be informed about Service Requests created by ASR.

2.4 Oracle Partner Network (OPN) Partners and ASR

If support services for your ASR assets are provided by an Oracle Partner, the Partner is responsible for ASR activation in My Oracle Support. When ASR detects a fault, only the Partner is notified of the problem.

ASR generates a draft Service Request in My Oracle Support, accessible only to the Partner. If the Partner requires assistance from Oracle Support to resolve the problem, they use My Oracle Support to promote the draft Service Request to a technical Service Request.

The Partner's My Oracle Support account *must* have access to their respective partner Customer Support Identifier (CSI) **and** the customer's CSI associated with the asset and must have administrator privileges on **both** CSIs. The Partner has the responsibility to:

- Use My Oracle Support to:
 - Assign contacts to ASR assets. The contact must be a member of the Partner's organization, and the MOS account must be associated with the Partner's CSI.
 - [optional] Assign distribution email addresses to ASR assets. This can be used to send ASR email notifications to an email list maintained by the Partner.
 - Activate ASR assets.
 - Maintain ASR asset information.
- Provide a Sun Online Account username and password to register the ASR Manager, using a Partner email address.
- Provide service to their customers when ASR detects problems.

You can use My Oracle Support to view ASR asset status, but you cannot edit the ASR asset information.

Install the ASR Manager

This chapter explains how to install the ASR Manager, which must be installed first before ASR Assets. Installing the ASR Manager consists of the following tasks:

1. Install Service Tags
2. Check for Oracle Automated Service Manager (OASM) installation and version
3. Download the latest OASM and ASR packages
4. Install the OASM and ASR packages
5. Register and verify the ASR Manager
6. Configure Crontab

Note: An ASR Manager can be activated as an ASR asset, if it is qualified for ASR and entitled to service. In this case, you must select your ASR Manager from the list of qualified hardware (see <http://www.oracle.com/asr>). Once you install and register the ASR Manager as described in this chapter, complete the instructions in "Configure and Manage ASR Assets".

3.1 Prerequisite Tasks

The following tasks should already be complete before the ASR Manager is installed:

- Verify access to My Oracle Support (login and password).
- Assess ASR Systems (see "Oracle Auto Service Request Configuration Requirements" on page 1-7 and "Telemetry Sources: Overview and Check" on page 1-10) (OS version check, network validation, JDK version check, verify existing telemetry sources).

Because the ASR Manager no longer requires being installed on a device that is currently under an Oracle Service Contract *and* that the server has been qualified for ASR, you now have more flexibility regarding how you can install ASR. Some of the possibilities include:

- x86 or SPARC Server running Solaris 10u6 or later
 - local zone

Note: If the ASR Manager is installed on a local zone, it is not possible to activate the ASR Manager as an ASR asset. If this is attempted, an error will be received: *Asset cannot be activated due to unknown product name or serial number*. This is a known issue expected to be corrected in a future version of Oracle ASR.

- SPARC Server running Solaris 10u6 or later
 - logical domains
- x86 Server running Oracle Linux 5.3 or later
- Windows 7/Windows XP
 - VirtualBox running Solaris 10u6 or later
 - VirtualBox running Oracle Linux 5.3 or later
- Installation on M-Series domains and blade servers

Note: Oracle Linux runs on x86 servers, and logical domains are specific to Solaris SPARC servers

The ASR Manger still has to be registered but no longer has to be activated as an ASR Asset. The requirement that the ASR Manager has to be activated for ASR before activating other ASR Assets has also been lifted.

An ASR Manager can still be activated as an ASR Asset, if it is qualified for ASR and entitled to service.

3.2 Install Service Tags

This section provides instructions for downloading the appropriate software to enable service tags for Solaris and Oracle Linux systems.

3.2.1 Install Service Tools Bundle (STB) for Solaris

Note: If your ASR Manager system is running Solaris 11, the installation of STB is not required. See "[Enable the HTTP Receiver for Solaris 11 ASR Assets](#)" on page 3-7.

STB is a tool set that helps ASR obtain required information from each ASR system before you can activate them, such as obtaining the system's serial number from firmware. Follow the instructions below to install the Service Tools Bundle (STB) v6.0 or later.

Note: If your system is using only a service processor-based telemetry source (ILOM, or XSCF on M-Series), STB does not need to be installed. If this is your situation, go to "[Install the ASR Package](#)" on page 3-6.

1. On the system where ASR is to be installed, open a terminal window and log in as root.
2. Download the latest Oracle Service Tool Bundle (STB) software (login to My Oracle Support and see Doc ID 1153444.1). This document includes the download links organized by platform. Click the link that corresponds to your platform.

Note: If needed, log in to another machine to complete the download and then copy the file to the system targeted for ASR installation.

3. Click the `install_stb.sh.tar` file to download it
4. Untar the file from the download directory:


```
tar -xvf install_stb.sh.tar
```
5. Execute the resulting file. You may have to change shells to `sh` if the file does not execute. Also, you may have to set execute permissions on the file, as shown below:

```
sh
chmod +x install_stb.sh
./install_stb.sh
```

Note: STB will install all applications bundles by default. You can downgrade applications when invoked with the `-force` option in non-interactive mode. Run `install_stb.sh -?` to view all installation options.

6. STB version 6.0 and higher defaults to installing all tools, a "yes" (y) response is already selected for you. As the installation progresses, you will be prompted for confirmation that you wish to install the tools.

When prompted: "Would you like to (I)nstall, (X)tract component selections, or (E)xit," press [Enter].

7. To confirm that STB is installed correctly, and that it is reporting your system's serial number correctly, run:


```
sneep -a
```
8. If the serial number for your system is not displayed, run the command below to set the serial number. Keep in mind that the definitive source for the actual serial number is on the chassis of your system. It should also be the same in the My Oracle Support database, as described in "[Review Assets in My Oracle Support](#)" on page 2-2.


```
sneep -s [serial_number]
```
9. Run the following command to be sure that STB is reporting your system attributes correctly:


```
stclient -Ex
```
10. Be sure that the following attributes are reporting as indicated:
 - `<agent_version>` must be **5.2** or above
 - `<system>` must be **SunOS**

- `<platform>` must be your platform type
 - `<serial_number>` must be the serial number of your system
 - `<product_name>` must be **Solaris Operating System**
 - `<container>`global
`<source>` must be **SUNWstosreg**
 - `<container>`global
`<source>` must be **SUNWsthwreg**
11. If you are not getting the correct data, re-install STB.
 12. Proceed to "[Install the ASR Package](#)" on page 3-6.

3.2.2 Install Service Tags for Oracle Linux

1. Download and unzip the latest Sun Service Tags .zip file. You can download Sun Service Tags 1.1.5 from:

<https://updates.oracle.com/download/12757884.html>

Note: The Sun Service Tags are only required for an ASR Manager system that is also identified as an ASR Asset.

2. Run the following commands to install the service tags:

```
rpm -i sun-servicetag-1.1.5-1.i386.rpm
rpm -i sun-hardware-reg-1.0.0-1.i386.rpm
```

3. Proceed to "[Install the ASR Package](#)" on page 3-6.

Note: JDK 6 is required for OASM. You can download the latest version from the Java SE Downloads page (see: <http://www.oracle.com/technetwork/java/javase/downloads/jdk6-jsp-136632.html>)

3.3 Check for OASM Installation and Version

Follow the procedure below to determine if you already have OASM installed. For more information on the relationship between OASM and ASR, refer to "[Close-Up of the ASR Manager](#)" on page 1-3.

1. Open a terminal window to the system where the ASR Manager is to be installed and log in as root.
2. Run the following command to determine the existence and version of OASM:
 - For Solaris, run: `pkginfo -l SUNWsasm`
 - For Oracle Linux, run: `rpm -q SUNWsasm`
3. Make note of the results and continue to the next section.

Note: OASM on Oracle Linux will add a crontab on install to check that `sasm` is running. The default values are to check every 12 minutes.

3.4 Download the OASM and ASR Packages

If you do not have Oracle Automated Service Manager (OASM) installed, follow the procedure below to download both the OASM and ASR packages.

1. From the machine where the ASR Manager is to be installed, open a terminal window and make sure you are logged in as root.
2. In a browser, click the following links to download OASM and ASR packages. You must login to My Oracle Support (<https://support.oracle.com>). See Document ID 1185493.1 for the software download links for OASM and ASR.

Note: If a browser is not available, download the files to another machine and copy them to the machine where the ASR Manager is to be installed.

3. Once the file(s) are downloaded, go to the download directory, or other directory where you copied the .zip file(s), and unzip the file(s). Be certain that the file(s) are copied to an installation directory on the system where the ASR Manager is to be installed before unzipping them.
4. If you do not need to install OASM, skip the following procedure and go to "[Install the ASR Package](#)" on page 3-6. Otherwise, continue to the following procedure.

3.5 Install the OASM Package

Follow the procedure below to install OASM.

Note: OASM is installed on the ASR Manager system only, not ASR Assets.

1. Open a terminal window and make sure you are logged in to the ASR Manager system as root.
2. From the directory where you unzipped the OASM package, install the OASM package using the following command:
 - For Solaris, run: `pkgadd -d SUNWsasm.version_num.pkg`
 - For Oracle Linux, run: `rpm -i SUNWsasm.version_num.rpm`

Note: See "[Installing ASR Manager on Blade Systems](#)" on page 6-8 for additional information on installing the ASR Manager on a blade system.

3. As the installation progresses, you are prompted to make several selections. Use the list below to determine how to respond to the installation prompts:
 - When prompted: “. . . install all packages,” press **[Return]**.
 - When prompted: “. . . install conflicting files,” enter **Y**.
 - When prompted: “. . . scripts will be executed with super-user permission during the process of installing this package,” enter **Y**.

4. Once the installation completes successfully, continue to ["Install the ASR Package"](#).

Run the following command to get the status of the OASM process ID (PID):

- For Solaris: `svcs sasm`
- For Oracle Linux: `/opt/SUNWasm/bin/sasm status`

3.6 Install the ASR Package

Follow the procedure below to install the ASR package on the ASR Manager system.

1. Open a terminal window and make sure you are logged in to the ASR Manager system as root.
2. From the directory where you unzipped the ASR package, install the ASR package using the following command:
 - For Solaris, run: `pkgadd -d SUNWswasr.version_num.pkg`
 - For Oracle Linux, run: `rpm -i SUNWswasr.version_num.rpm`
3. As the installation progresses, you are prompted to make several selections. Use the list below to determine how to respond to the installation prompts:
 - When prompted: ". . . select all packages to process," press **[Return]** to select all packages.
 - When prompted: ". . . install conflicting files," enter **Y**.
 - When prompted: ". . . scripts will be executed with super-user permission during the process of installing this package," enter **Y**.
4. Add the `asr` command to the PATH (update to the root's `.profile`, `.cshrc`, `.kshrc`, or `.bashrc` files as needed) (for both Solaris and Oracle Linux):
 - `PATH=$PATH:/opt/SUNWswasr/bin`
`export PATH`
5. To confirm proper network connectivity between the ASR Manager and Oracle, go to ["Test Connectivity from the ASR Manager to Oracle"](#) on page 5-13. When complete, continue to the next procedure ["Register the ASR Manager"](#).

3.7 Register the ASR Manager

Follow the procedure below to register the ASR Manager (for both Solaris 10u6, Solaris 11, and Oracle Linux machines). Make sure you are logged in to the ASR Manager system as root.

1. To register the ASR Manager, run: `asr register`
2. If you are using a proxy server for access to the internet, enter the proxy server information as you determined in ["ASR Manager Network Connection Requirements"](#) on page 1-9. If you are not using a proxy server, enter: `-` (hyphen).

Note: If you are using a SOCKS proxy, enter the hyphen - for no proxy. When completed with the steps in this procedure, manually edit the OASM `config.ini` file with your SOCKS proxy server information. For instructions, refer to "[Configure ASR to Send HTTPS Traffic Through a Proxy Server](#)" on page 5-12. If you are using an NTLM proxy, pay close attention to the requirements as shown in the installation prompts (shown below). You may have to contact a network administrator for assistance.

3. Screen output should look like this:

```
Proxy server name: ? <proxy server name>
Proxy port number: ? <proxy port number>
Proxy authentication; if authentication is not required, enter -.
Proxy user: <proxy user name>
Proxy password: <proxy password>
If this is an NTLM type proxy, enter the information below.
Otherwise, enter -
NTLM Domain: [?] <NTLM domain name>
Enter the host the NTLM authentication request is originating
from. Usually this is the hostname of the SASM server.
NTLM Host: [?] <NTLM host name>
NTLM support is not bundled with SASM but may be added now.

1) Download jCIFS from http://jcifs.samba.org/
2) Extract contents and locate the jcifs-*.jar file
3) Enter full path to this file below

jCIFS jar file: [?] <full path of jCIFS jar file>
Note: These properties are stored in the
/var/opt/SUNWsasm/configuration/config.ini file. You can update these
properties if needed and then restart the SASM.
```

4. Enter the username and password of your My Oracle Support account when prompted.
5. Upon entry of your My Oracle Support credentials, ASR will validate the login. Once validated, the registration is complete.
6. Check the registration status of ASR. Run: `asr show_reg_status`
A message is displayed on the screen indicating whether ASR is registered with the transport server.
7. To be sure that ASR can send information to the transport server, run:
`asr test_connection`

This command sends a test message (ping) to the transport server.
8. Upon successful results of the above commands, the registration of the ASR Manager is complete.

3.8 Enable the HTTP Receiver for Solaris 11 ASR Assets

Solaris 11 includes the ability to send ASR fault events and telemetry to Oracle using xml over HTTP to the ASR Manager.

To enable this capability, use the `asr enable_http_receiver` command. Select a port for the HTTP receiver that is appropriate for your network environment and does not conflict with other network services.

Follow the procedure below to enable the HTTP receiver for Solaris 11 ASR Assets. Make sure you are logged in to the ASR Manager system as root.

1. After installing ASR 3.5 or later, enable the HTTP receiver:

```
/opt/SUNWswasr/bin/asr enable_http_receiver -p <port_number>
```

Note: If you need to disable the HTTP receiver, run:

```
/opt/SUNWswasr/bin/asr disable_http_receiver
```

2. Verify the HTTP receiver is up and running. In a browser, go to:

```
http://<asr_manager_host>:<port_number>/asr
```

A message will display indicating that the HTTP receiver is up and running.

If you need to use HTTPS for security purposes, you can set up HTTPS/SSL for the ASR Manager HTTP receiver:

1. The detailed steps for enabling https/SSL for Jetty are documented at <http://docs.codehaus.org/display/JETTY/How+to+configure+SSL>
2. Once the SSL certificate from a trusted authority is loaded into keystore, then add the following SSL connector in

`/var/opt/SUNWsasm/configuration/jetty/jetty.xml` below the `<Call name="addConnector">` sections:

```
<Call name="addConnector">
  <Arg>
    <New class="org.mortbay.jetty.security.SslSocketConnector">
      <Set name="Port">443</Set>
      <Set name="maxIdleTime">30000</Set>
      <Set name="keystore">/path/to/keystore</Set>
      <Set name="password">...</Set>
      <Set name="keyPassword">...</Set>
      <Set name="truststore">/path/to/keystore</Set>
      <Set name="trustPassword">...</Set>
    </New>
  </Arg>
</Call>
```

Passwords above can be plain text or obfuscated as follows:

```
java -classpath lib/jetty-6.1.7.jar:lib/jetty-util-6.1.7.jar
org.mortbay.jetty.security.Password <plaintext-password>
```

Then copy/paste the output line starting with `OBF:` (including the `OBF:` part) into this `jetty.xml` config file.

3. Restart OASM:
 - Solaris: `svcadm restart sasm`
 - Oracle Linux: `/opt/SUNWsasm/bin/sasm stop-instance` and then run `/opt/SUNWsasm/bin/sasm stop-instance`
4. Verify the SSL setup by accessing the following URL from a browser:

`https://<asr_manager_host>/asr`

3.9 Set Up Crontab

Crontab entries are automatically created when the ASR Manager is installed. These crontab entries perform the following tasks:

- asr heartbeat:** This task sends a message to the Oracle backend server every 12 hours. If the Oracle/ASR back-end systems do not receive the heartbeat in 48 hours, they send an email to the My Oracle Support account's technical contact used to install/register the ASR Manager. Refer to "[ASR Emails](#)" on page 5-9 for more information.

Note: The ASR Manager must be configured correctly to send the daily cron job for asr heartbeat. Failure to do so will result in the unit being marked as a 'Heartbeat Failure' unit.

If an ASR Manager is in Heartbeat Failure mode for 90 days, it will be automatically deactivated at the ASR backend and in My Oracle Support. Also, any assets that are configured via that ASR Manager will also be marked deactivated. This will prevent any future events creating automatic Service Requests.

You can check to see if any ASR Manager or ASR Asset are in *Heartbeat Failure* by reviewing the ASR status in My Oracle Support.

- asr update_rules:** ASR uses fault rules to filter the telemetry data sent from ASR Assets. This filtering is done to remove telemetry that contains no real fault data and general telemetry "noise." The filtering process also ensures that telemetry that contains faults is reported. These fault rules can change as ASR improves its filtering and as new platforms and telemetry sources are supported by ASR. ASR installs a cron job on the ASR Manager system to periodically check Oracle's autoupdate server for any new rules updates. When there are new rules, the ASR Manager automatically downloads and installs the latest rules bundle. If the crontab entry for automatic rules updates is disabled, then you will receive an e-mail, which will be sent to the email address associated with the MOS account used to register the ASR Manager, to notify you that updated rules are available. For more information on fault rules, refer to "[ASR Emails](#)" on page 5-9.

Note: If the **asr heartbeat** is disabled in crontab, you will not be notified, via email, if your ASR fault rules are out of date with the most current release. To be sure your fault rules are current, you can run the `asr update_rules` command from the ASR Manager system.

The crontab entries are set-up as follows and can be changed by the ASR installer as needed:

```
asr heartbeat: 0 0,12 * * * /opt/SUNWswasr/bin/asr heartbeat
```

```
asr report: 0 6 1 * * /opt/SUNWswasr/bin/asr report
```

```
update rules: 0 <random number between 1-59> 0 <random number between 1-23>  
* * * /opt/SUNWswasr/bin/update_rules.sh
```

Configure and Manage ASR Assets

This chapter provides the instructions to configure ASR Assets. Keep in mind that an active ASR Manager must be installed before configuring ASR Assets. Before continuing, the following prerequisites must be complete for the system(s) targeted for ASR configuration:

- Verify access to My Oracle Support.
- ["Review Assets in My Oracle Support"](#) on page 2-2. The system serial number must be in the My Oracle Support database, have an active contract, and an assigned technical contact.
- ["Oracle Auto Service Request Configuration Requirements"](#) on page 1-7 (OS version check, network validation, verify existing telemetry sources).

Note: If you want to use the ASR Manager as an asset, too, then telemetry reporting will need to be configured.

If you have completed installing the ASR Manager and need to set-up telemetry reporting on the ASR Manager, go to ["Telemetry Sources: Overview and Check"](#) on page 1-10.

4.1 Install Service Tools Bundle (STB)

You may need to install the Service Tools Bundle (STB) software on your ASR Asset system. Proceed to the following instructions in order. When complete, return to these instructions. See ["Install Service Tools Bundle \(STB\) for Solaris"](#) on page 3-2.

Note: If your ASR Asset system is running Solaris 11, then STB is not required to enable ASR telemetry. However, STB is required to enable Oracle proactive services.

4.2 Obtain the ASR Asset Bundle for non-ILOM Telemetry Sources

Note: If your ASR Asset system is running Solaris 11, then you can skip this section. See ["Activate and Register ASR Assets for Solaris 11 Systems"](#).

The ASR Asset Bundle includes a shell script for configuration ASR assets running Solaris. The script (`asrassetmenu.sh`) can be used to:

1. Check system for ASR requirements
2. Add a trap-destination to SunMC agent
3. Add a trap-destination to FMA agent
4. Remove a trap-destination from SunMC agent
5. Remove a trap-destination from FMA agent
6. List SunMC agent trap-destinations
7. List FMA agent trap-destinations
8. Test event to verify ASR connectivity

The ASR Asset bundle is not required on ILOM service processors and M-Series XSCF. To verify your system's telemetry, visit the Oracle Auto Service Request product page (<http://www.oracle.com/asr>).

If you are configuring an M-series system, skip this procedure and go to "[Enable M-Series XSCF Telemetry](#)" on page 4-6. In all other cases, follow the procedure below to obtain the ASR Asset bundle.

1. Open a terminal window and log in as root on the system where the ASR Manager is installed.
2. Go to `/opt/SUNWswasr` and copy the `ASRAssetBundle.version_num.tar` file to all systems that will be ASR Assets. You can copy the file to an NFS location or use a provisioning tool to distribute the file to a group of assets. Copy the ASR Asset Bundle file to any directory on the system, such as `/opt` or `/tmp`.
3. Open a terminal window and log in as root on the ASR Asset system.
4. Go to the directory where you copied the ASR Asset Bundle file and unzip and untar the `ASRAssetBundle` (for qualified Solaris systems only):

```
tar -xvf ASRAssetBundle.version_num.tar
```

4.3 Set Up Telemetry Sources to ASR

These procedures enable telemetry sources on your system(s) to send telemetry to Oracle. These steps are the same for both the ASR Manager and ASR Assets. Before continuing, you should have already verified what telemetry sources reside on the system, as explained in "[Telemetry Sources: Overview and Check](#)" on page 1-10. Depending upon what telemetry sources reside on your system, complete one or more of the following procedures:

- "[Enable FMA Telemetry for Solaris 10 ASR Assets](#)"
- "[Enable FMA Telemetry for Solaris 11 ASR Assets](#)"
- "[Enable ILOM Telemetry](#)"
- "[Enable M-Series XSCF Telemetry](#)"

4.3.1 Enable FMA Telemetry for Solaris 10 ASR Assets

If your ASR Assets run Solaris 11, then see "[Enable FMA Telemetry for Solaris 11 ASR Assets](#)". Follow the procedure below to enable FMA telemetry sources for a Solaris 10 ASR Asset:

1. Make sure you are logged in as root on the system whose telemetry you wish to enable. This could be either an ASR Manager or an ASR Asset system.

2. Go to the directory where you untarred the Asset Bundle file, and then go to the specific ASR Asset Bundle directory. For example:

- On an ASR Asset: `cd /file_copy_location/asrassetbundle`
- On an ASR Manager: `cd /opt/SUNWswasr/asrassetbundle`

3. Launch the ASR Asset menu. Run `./asrassetmenu.sh` to display the menu:

```
Welcome to the ASR asset menu
-----
1) Check system for ASR qualifications
2) Add a trap-destination to SunMC agent
3) Add a trap-destination to FMA agent
4) Remove a trap-destination from SunMC agent
5) Remove a trap-destination from FMA agent
6) List SunMC agent trap-destinations
7) List FMA agent trap-destinations
8) Test event to verify ASR connectivity
9) Exit
```

4. Select 3 to enable FMA telemetry. Respond to the script's prompts as follows:

- When prompted, "Please enter Hostname or IP address of SASM ASR plugin," enter the information for the ASR Manager. Whether you are enabling telemetry on the ASR Manager system or on ASR Asset systems, the hostname or IP entered **must be for the installed ASR Manager**.
- When prompted, "Please enter SNMP port of SASM ASR plugin (q to quit) [162]," press **[Return]** or enter another port if you have changed your port settings for ASR
- When prompted, "Do you want to set trap-destination [y,n,q]," confirm the displayed information, enter **Y**, and press **[Return]**.

5. The ASR Asset Menu then enables the telemetry and displays where the telemetry from this system will be sent (IP or hostname of the ASR Manager).

6. Repeat for all ASR Assets.

7. When complete, enable any other telemetry sources that may reside on the system (for example, ILOM). Refer to ["Set Up Telemetry Sources to ASR"](#) on page 4-2, if required, and return to these instructions.

8. If you have enabled all telemetry sources on an ASR Asset system, go to ["Activate ASR Assets"](#) on page 4-7.

4.3.1.1 Command Line Options for Setting Solaris FMA Trap Destinations

You can incorporate ASR asset configuration into your automated provisioning process. The `asrassetmenu.sh` script now includes command line options for setting Solaris FMA trap destinations. To set a Solaris FMA trap destination from the command line:

```
asrassetmenu.sh -solaris <destination_IP_address> <port_number>
```

The `asrassetmenu.sh` script will exit with an error status value for any of these conditions:

- `<destination_IP_address>` not provided
- `<port_number>` not provided
- Trap destination unable to be set

4.3.2 Enable FMA Telemetry for Solaris 11 ASR Assets

Configuration and activation of Solaris 11 ASR Assets are performed concurrently. See "[Activate and Register ASR Assets for Solaris 11 Systems](#)".

4.3.3 Enable ILOM Telemetry

Follow the procedure below to enable ILOM telemetry. It is assumed that a network connection to the platform's dedicated service processor (SP) is connected and configured, as discussed in "[ILOM General Procedures](#)" on page 1-11. Do not continue with the installation unless you have confirmed the initial ILOM set-up. Additionally, you will need the ILOM service processor IP address to complete the following procedure.

4.3.3.1 Enable ILOM: GUI Interface

ASR installers have the choice of using a web-based GUI or a command-line interface to enable ILOM telemetry. Follow the procedure below for the GUI method. If command-line is desired, go to "[Enable ILOM: Command Line Interface](#)".

1. From a web browser, access the IP address of the ILOM interface (note: **https**):
`https://IP_Address_of_ILOM_Interface`
2. Log in as root.
3. From the menu, select **Configuration**, then select **Alert Management**.

Note: If using ILOM on a Sun Blade 6000 series, select CMM from the left navigation pane, then select **Configuration**, and **Alert Management**.

4. The Alert Setting screen lists 15 possible Alert IDs that can be configured to send ILOM telemetry. Alert ID slots that are occupied by existing alert settings are shown along with their alert parameters. Choose an Alert ID that is not used by selecting the radio button next to the Alert ID number.

Note: Unused Alert IDs are mainly indicated by the disable setting in the **Level** column and by all zeros in the **Destination Summary** column.

5. Select **Edit** from the **Actions** pull-down menu.

Note: If using ILOM on a Sun Blade 6000 series, select the **Edit** button from the top of the screen.

6. Enter data in this screen as follows:
 - **Level:** Select **Minor** from the pull-down menu. If removing an ILOM trap, select **Disable**.
 - **Type:** Select **SNMP Trap** from the pull-down menu.
 - **IP Address:** Enter the **IP Address** of the ASR Manager system.

- **Destination Port:** The default of 0 is automatically set, meaning that the port is assigned to the default for SNMP (**162**). For ILOM versions 2.0.4.2 or lower, the port cannot be changed from the default.
 - **SNMP Version:** Select **v2c** from the pull-down menu.
 - **Community Name:** Enter **public** in the text entry field.
7. Click the **Save** button.
 8. Generate test alerts. In the *Alert Settings* page, select the alert you want to test and then click the **Send Test Alert** button. ILOM generates a test event for the selected alert. If configured properly, you will receive a test Service Request e-mail.
 9. Repeat for each ASR Asset required for ILOM telemetry.
 10. If you have enabled all telemetry sources on an ASR Asset system, go to "[Activate ASR Assets](#)" on page 4-7.

4.3.3.2 Enable ILOM: Command Line Interface

Follow these ILOM command line procedures below to enable ILOM telemetry. If you used the GUI method, as described in the previous procedure, you do not need to complete these steps.

1. Open a terminal window and `ssh` to the IP address of the ILOM network interface:


```
ssh IP_address_of_ILOM_interface
```
2. Log in as root.
3. Before enabling ILOM telemetry, it is important to understand that ILOM supports up to 15 user-configurable alert rules. It is one of these rules you must set to enable ILOM telemetry. Therefore, you must first choose one of these rules (1 to 15) to set. Before choosing, however, you must determine that the rule you select is not currently being used. You can use the web-based GUI method to determine this quickly, as discussed in "[Enable ILOM: GUI Interface](#)". Otherwise, run the following command to determine an available alert rule slot.
 - For Rack Mount Servers and Blades:


```
-> show /SP/alertmgmt/rules/x
```
 - For the Sun Blade 6000 Chassis:


```
-> show /CMM/alertmgmt/rules/x
```

Important: Substitute *x* for a rule number (1 to 15). If you see that a rule level is set to anything else but disabled, the alert rule slot is occupied. Rerun the command above and substitute the rule number with the next number in sequence (for example, 2, then 3, etc.) until you find an available alert rule slot.

4. Once an alert rule slot is determined, run one of the following commands. Pay close attention to the following data entry points before running the command:
 - **rules/x:** For *x*, enter a number from **1** to **15**, depending upon which alert rule slot you have determined is unoccupied using the previous step.
 - **destination:** Enter the IP address of the **ASR Manager**.

- **destination_port:** The port is assigned to the default for SNMP (162). For ILOM versions 2.0.4.2 or lower, the port cannot be changed from the default. For ILOM versions higher than 2.0.4.2, the destination port can be changed if needed. If you wish to change the port, add the `destination_port=xxx` parameter into the command following the destination parameter.

Note: If you are removing a trap, set the level parameter to `disable`.

- For Rack Mount Servers and Blades:

```
-> set /SP/alertmgmt/rules/x type=snmptrap level=minor destination=IP_of_ASR_Manager snmp_version=2c community_or_username=public
```

- For the Sun Blade 6000 Chassis:

```
-> set /CMM/SP/alertmgmt/rules/x type=snmptrap level=minor destination=IP_of_ASR_Manager snmp_version=2c community_or_username=public
```

5. Generate test alerts. Type one of the following command paths to set the working directory:

- For a rack-mounted server SP, type: `cd /SP/alertmgmt/rules`
- For a blade server SP, type: `cd /CH/BLn/SP/alertmgmt/rules`
- For a chassis CMM, type: `cd /CMM/alertmgmt/CMM/rules`

Type the following command to generate a test alert:

```
->set testalert=true
```

6. If configured properly, you will receive a test Service Request e-mail.
7. Repeat this process (steps 1 through 6) for each ASR Asset using ILOM telemetry.
8. If you have enabled all telemetry sources on an ASR Asset system, go to "[Activate ASR Assets](#)" on page 4-7.

4.3.4 Enable M-Series XSCF Telemetry

Follow the procedures below to enable M-Series XSCF telemetry. It is assumed that a network connection to the platform's dedicated service processor (SP) is connected and configured. Do not continue with the installation unless you have confirmed the initial XSCF set-up.

Note: This procedure can also be used to remove XSCF trap destinations. For more information on XSCF, refer to the *XSCF User Guide for SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers*.

1. Open a terminal window and initiate an `ssh` connection to the IP address of the XSCF network interface:

```
ssh IP_address_of_XSCF_interface
```

2. Log in to the XSCF console. Make sure you have `platadm` privileges, (run `showuser -p <login name>`). You can run `showuser -p` for a list of users with this privilege.
3. Disable the SNMP agent:


```
XSCF> setsnmp disable
```
4. Add the ASR Manager system as the trap destination. If using these procedures to remove a trap, see further below in this step:


```
XSCF>setsnmp addtraphost -t v2 -s public -p 162 xxx.xxx.xxx.xxx
```

-s = community string (default value is **public**)
-p = SNMP listener port (default value is **162**)
`xxx.xxx.xxx.xxx` = ASR Manager IP address

If you wish to remove an XSCF trap destination, run the following command to stop XSCF from sending telemetry to the ASR Manager system:

```
XSCF>setsnmp remtraphost -t v2 xxx.xxx.xxx.xxx
```

`xxx.xxx.xxx.xxx` = ASR Manager IP address
5. Enable the SNMP agent:


```
XSCF> setsnmp enable
```
6. Enable SNMP v1v2:


```
XSCF> setsnmp enablev1v2c <community>
```

community is the community string and should always be set to **public**.
7. Verify SNMP settings to make sure the trap destination is set and SNMP is enabled.


```
XSCF> showsnmp
```

```
Agent Status: Enabled
Agent Port: 161
System Location: Unknown
System Contact: Unknown
System Description: Unknown
Trap Hosts:
Hostname Port Type Community String Username Auth Protocol
xxx.xxx.xxx.xxx 162 v2 public n/a n/a
SNMP V1/V2c:
Status: Enabled
Community String: public
Enabled MIB Modules:
SP MIB
FM MIB
```
8. Repeat for each M-Series ASR Asset required for XSCF telemetry.
9. If you have enabled all telemetry sources on an ASR Asset system, go to ["Activate ASR Assets"](#).

4.4 Activate ASR Assets

Follow the procedures below to activate ASR Assets. Once ASR Assets are activated, the configuration of the ASR Assets is complete. All assets to be activated should already have telemetry trap destinations set, as described in ["Set Up Telemetry Sources to ASR"](#) on page 4-2. If this has not been done, complete that task first before

continuing. Proceed to one of the following options, depending upon your circumstance:

- If you are activating a Sun Blade system, go to ["Activate Blade Assets"](#) on page 4-9 to activate the system.
- If you are activating an Exadata system, go to ["Activate Exadata Assets"](#) on page 4-11 to activate the system.
- If you are activating ASR Asset systems that run Solaris 11, go to ["Activate and Register ASR Assets for Solaris 11 Systems"](#) on page 4-12.
- For all other systems, use the procedure below:
 1. Open a terminal window and log in as root on the ASR Manager system.
Important: Activating ASR Assets is not done on the assets themselves but on the ASR Manager system only.
 2. Run the following activate command for each ASR Asset. Be sure to use the IP or hostname of the ASR Asset system.


```
asr activate_asset -i <IP address>
or
asr activate_asset -h <hostname>
```
 3. Login to My Oracle Support to complete the activation process. See ["Enable ASR Assets in My Oracle Support"](#) on page 2-3 for details.
 4. While you are logged into My Oracle Support, you can view your ASR Assets. In the My Oracle Support Dashboard, click the "More..." tab. Then select "Settings" from the menu.
 5. In the "Settings" pane on the left of the window, select "Assets" (located under the Administrative submenu). A complete list of all ASR Assets is displayed:

Serial Number	Asset Name	Product Name	Host Name	Support Identif...	Contact Name	ASR Status
0948	Cores2	S7410 Family	cores2-ar1	17	Carl	Active
07	Wayne Seltzer ...	SFV215,1x1.5,1...		17	Wayne Seltzer	Active
06		X4100 M2:2x222...		17	Jason	Active
060		X4100:2x252 4x1...	ASR-Asset2	17	Angelo	Active
07	Wayne Seltzer	SFV215,1x1.5,1...	unknown	17	Wayne Seltzer	Active - No Heartbeat
072		SE T5220 BASE ...		17		Pending
072		SE T5120 BASE ...		17		Pending
084		X4240:1x2347HE...		17		Pending
092		X2270:1xE5540,...		17		Pending
228		SFV880 4@900 ...		17		Pending
338		280R/2x1.2GHz/...		17		Pending
BEL		SE T5120 8CR 1....		17		Pending
BEL		FJ T5120 4CR 1....	unknown	17		Pending
FMS		SFV210,1x1GHz,...		17		Pending

Note: Auto Activation: If the ASR Manager receives fault telemetry from an asset that has not been previously activated, ASR automatically attempts to activate the asset as if the `asr activate_asset` command is executed.

4.4.1 Activate Blade Assets

Use the following procedure to activate a Sun Blade system. Keep in mind that Blade systems also include the chassis within which the Blade systems are installed. Therefore, when activating, the Blade and the chassis must be activated. Chassis telemetry reports power and environmental faults, and blade telemetry reports faults specific to the blade's subsystems. You will need the IP addresses of the Blade chassis and the Blade systems in order to complete this procedure.

4.4.1.1 New ASR Activation on Blade Systems and Chassis

1. Open a terminal window and log in as root on the ASR Manager system.
Important: Activating ASR Assets is not done on the assets themselves but on the ASR Manager system only.
2. Run the following commands. If activating an X6270 or X6275 system, see the note further below.

```
asr activate_asset -i Chassis_ILOM_IP
asr activate_blade -i Blade_IP -c Chassis_ILOM_IP
```

3. Repeat the `asr activate_blade` command for each Blade within the chassis that you desire to have under ASR management. Keep in mind that the Blade systems must be qualified for ASR, as specified in the "Systems Qualified for ASR" link at: <http://oracle.com/asr>

Note: For the X6270, the `asr activate_blade` command is issued twice. It is issued once where Blade IP is the IP of the blade's service processor, and once where Blade IP is the IP of the blade's host. The host of an X6270 or X6275 can only be activated if it is running Solaris. It is acceptable to only activate the service processor of the blade in this case. The ILOM on the service processor for an X6270 must be configured.

4. Login to My Oracle Support to complete the activation process. See "[Enable ASR Assets in My Oracle Support](#)" on page 2-3 for details.
5. While you are logged into My Oracle Support, you can view your ASR Assets. In the My Oracle Support Dashboard, click the "More..." tab. Then select "Settings" from the menu.
6. In the "Settings" pane on the left of the window, select "Assets" (located under the Administrative submenu). A complete list of all ASR Assets is displayed:

Serial Number	Asset Name	Product Name	Host Name	Support Identif...	Contact Name	ASR Status
0948	Cores2	S7410 Family	cores2-ar1	17	Carl	Active
07	Wayne Seltzer ...	SFV215,1x1.5,1...		17	Wayne Seltzer	Active
06		X4100 M2:2x222...		17	Jason	Active
060		X4100:2x252 4x1...	ASR-Asset2	17	Angelo	Active
07	Wayne Seltzer	SFV215,1x1.5,1...	unknown	17	Wayne Seltzer	Active - No Heartbeat
072		SE T5220 BASE ...		17		Pending
072		SE T5120 BASE ...		17		Pending
084		X4240;1x2347HE...		17		Pending
092		X2270;1xE5540,...		17		Pending
228		SFV880 4@900 ...		17		Pending
332		280R/2x1.2GHz/...		17		Pending
BELL		SE T5120 8CR 1...		17		Pending
BELL		FJ T5120 4CR 1...	unknown	17		Pending
FMS		SFV210,1x1GHz,...		17		Pending

4.4.1.2 Previously ASR-Activated Blade Systems

If you have previously activated a Blade chassis, follow these instructions to activate Blade systems.

1. Open a terminal window and log in as root on the ASR Manager system.
Important: Activating ASR Assets is not done on the assets themselves but on the ASR Manager system only.
2. Run the following command. If activating an X6270 or X6275 system, see the note further below.

```
asr activate_blade -i Blade_IP -c Chassis_ILOM_IP
```

3. Repeat the `asr activate_blade` command for each Blade within the chassis. Keep in mind that the Blade systems must be qualified for ASR, as specified in the “Systems Qualified for ASR” link at: <http://oracle.com/asr>

Note: For the X6270, the `asr activate_blade` command is issued twice. It is issued once where Blade IP is the IP of the blade’s service processor, and once where Blade IP is the IP of the blade’s host. The host of an X6270 or X6275 can only be activated if it is running Solaris. It is acceptable to only activate the service processor of the blade in this case. The ILOM on the service processor for an X6270 must be configured.

4. Login to My Oracle Support to complete the activation process. See "Enable ASR Assets in My Oracle Support" on page 2-3 for details.
5. While you are logged into My Oracle Support, you can view your ASR Assets. In the My Oracle Support Dashboard, click the “More...” tab. Then select “Settings” from the menu.
6. In the “Settings” pane on the left of the window, select “Assets” (located under the Administrative submenu). A complete list of all ASR Assets is displayed:

Serial Number	Asset Name	Product Name	Host Name	Support Identif...	Contact Name	ASR Status
0948	Cores2	S7410 Family	cores2-ar1	17	Carl	Active
07	Wayne Seltzer ...	SFV215,1x1.5,1...		17	Wayne Seltzer	Active
06		X4100 M2:2x222...		17	Jason	Active
060		X4100:2x252 4x1...	ASR-Asset2	17	Angelo	Active
07	Wayne Seltzer	SFV215,1x1.5,1...	unknown	17	Wayne Seltzer	Active - No Heartbeat
072		SE T5220 BASE ...		17		Pending
072		SE T5120 BASE ...		17		Pending
084		X4240;1x2347HE...		17		Pending
092		X2270;1xE5540,...		17		Pending
228		SFV880 4@900 ...		17		Pending
332		280R/2x1.2GHz/...		17		Pending
BEL		SE T5120 8CR 1...		17		Pending
BEL		FJ T5120 4CR 1...	unknown	17		Pending
FMS		SFV210,1x1GHz,...		17		Pending

4.4.1.3 Sun Blade X6275 Configuration

A Sun Blade X6275 server has two Service Processors that should be configured and activated for ASR using the steps described above. Also, each X6275 has two Hosts than can be configured as a secondary telemetry source.

- **Sun Blade X6275 Service Processors**

Activate each Sun Blade X6275 Service Processor with the command:

```
activate_blade -i <SP_IP_address> -c <CMM_IP_address>
```

When activated both X6275 Service Processors located on a single X6275 Blade Server will report ASR events independently. Each activated Service Processor on a single blade will be displayed in ASR as having the same serial number and a different IP address.

- **Sun Blade X6275 Hosts**

To use this telemetry each Host will need to be activated using the command:

```
activate_blade -i <Host_IP_address> -c <CMM_IP_address>
```

When activated both X6275 Hosts located on a single X6275 Blade Server will report ASR events independently. Each activated Host on a single blade will be displayed in ASR as having the same serial number and a different IP address.

4.4.2 Activate Exadata Assets

To activate Exadata assets, run the following command:

```
activate_exadata [-i exadataip -h exadatahostname -l ilomip] [-?]
```

or

```
activate_exadata [-i exadataip -h exadatahostname -n ilomhostname] [-?]
```

The parameters are:

- **-i exadataip** - The IP address of the database server host or storage cell.
- **-h exadatahostname** - The hostname of the database server host or storage cell.
- **-l ilomip** - The IP address of the ILOM corresponding to the database server host or storage cell.

- **-n ilomhostname** - The hostname of the ILOM corresponding to the database server host or storage cell.
- **-?** - Help (optional), displays help information.

Note: For details on enabling Oracle Auto Service Request on the Oracle Exadata servers, please refer to Oracle Exadata documentation.

4.4.3 Activate Exalogic Assets

To activate ASR on Exalogic OpenStorage Assets, use the embedded system management GUI. This is the same method for activating ASR on a standalone Sun Unified Storage 7xxx product.

To activate ASR on each Exalogic X4170 M2 server, use the `asr activate_asset` command from the ASR Manager. See [Enable ILOM Telemetry](#) to configure SNMP trap destinations on each of the ILOMs.

4.4.4 Activate and Register ASR Assets for Solaris 11 Systems

Follow the steps below to active ASR Assets for Solaris 11 systems:

1. Log in to the ASR Asset as the `root` user.
2. Enable the HTTP receiver for Solaris 11 ASR assets (see ["Enable the HTTP Receiver for Solaris 11 ASR Assets"](#) on page 3-7).
3. Run the following command to register the endpoint URL:

```
asradm register -e http://<asr_manager_host>:<port_number>/asr
```

4. Enter your Oracle SSO user name and password.
5. Log in to My Oracle support to complete the activation. See ["Enable ASR Assets in My Oracle Support"](#) on page 2-3.
6. Run the following command to view the status:

```
asradm list
```

The results should appear like this:

```
# asradm list
PROPERTY          VALUE
Status            Successfully Registered with ASR manager

System Id         <system identification number>
Asset Id          <asset identification number>
User              MyUserName
Endpoint URL      http://<asr_manager_host>:<port_number>/asr
#
```

7. To send a test e-mail, run the following command:

```
asradm send test <email.address@mycompany.com>
```

Your ASR Asset is now registered. You must complete the activation in My Oracle Support as described in ["Enable ASR Assets in My Oracle Support"](#) on page 2-3.

Note: If you need to unregister and deactivate your ASR asset, run:

```
asradm unregister
```

ASR Environment Administration

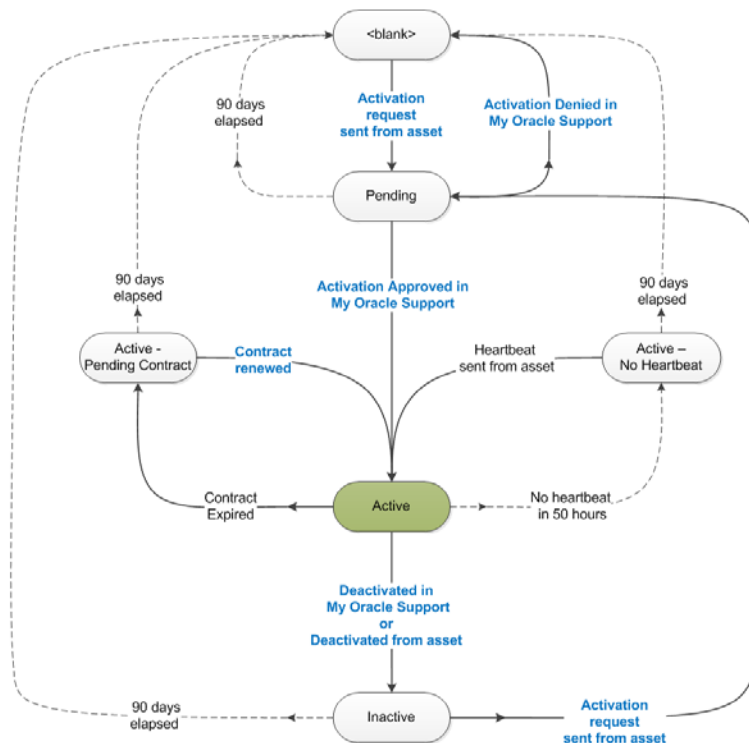
This chapter contains all procedures and other information required to manage the ASR environment.

5.1 ASR Asset Management

This section provides a variety of commands and procedures for managing ASR Assets. The following diagram shows the status transition of ASR Asset:

Auto Service Request (ASR) Asset Status transition diagram

Assets in My Oracle Support have an "ASR Status" value. This diagram illustrates how the ASR status changes when the user takes actions in the ASR asset's software and in My Oracle Support. The ASR asset status is also changed by automated actions of My Oracle Support and the ASR infrastructure. The initial ASR status value is <blank>.



5.1.1 View Status of ASR Asset(s) from the ASR Manager

The status of any ASR Asset can be obtained by running any one of the following command options from the ASR Manager system:

- `asr list_asset` - lists all assets associated with this ASR Manager
- `asr list_asset -i IP_Address_of_ASR Asset`
- `asr list_asset -h Hostname_of_ASR Asset`
- `asr list_asset -s Subnet_IP_Address_of_ASR Asset(s)`

Note: The `asr list_asset` command accepts a comma-delimited list of IP addresses, subnets, or hostnames.

The results will be similar to the following example:

IP ADDRESS	HOST NAME	SERIAL_NUMBER	ASR	PRODUCT_NAME
123.45.67.890	abcd.name.com	1234ABCD	Enabled	Sun-Fire-V240 SPARC
198.76.54.321	sasm-123-21	A11BAC	Enabled	Sun-Fire-V210 SPARC

5.1.2 Review Status of ASR Assets

To view the status of all ASR Assets, login to My Oracle Support (<https://support.oracle.com>). In the My Oracle Support Dashboard, click the "More..." tab. Then select "Settings" from the menu.

In the "Settings" pane on the left of the window, select "Assets" (located under the Administrative submenu). A complete list of all ASR Assets is displayed:

Serial Number	Asset Name	Product Name	Host Name	Support Identif...	Contact Name	ASR Status
0948000009	Cores2	S7410 Family	cores2-ar1	1710000000	Carl ...	Active
0700000000	Wayne Seltzer ...	SFV215,1x1.5,1...		1710000000	Wayne Seltzer	Active
0600000000		X4100 M2:2x222...		1710000000	Jason ...	Active
0600000003		X4100:2x252 4x1...		1710000000	Angelo ...	Active
0700000000	Wayne Seltzer	SFV215,1x1.5,1...	unknown	1710000000	Wayne Seltzer	Active - No Heartbeat
0720000000		SE T5220 BASE ...		1710000000		Pending
0720000000		SE T5120 BASE ...		1710000000		Pending
0840000000		X4240;1x2347HE...		1710000000		Pending
0920000000		X2270;1xE5540,...		1710000000		Pending
2280000000		SFV880 4@900 ...		1710000000		Pending
3380000000		280R/2x1.2GHz/...		1710000000		Pending
BELL000000		SE T5120 8CR 1...		1710000000		Pending
BELL000000		FJ T5120 4CR 1...	unknown	1710000000		Pending
FMS2000000		SFV210,1x1GHz,...		1710000000		Pending

5.1.3 Create Test Alert

The following command allows you to test the end-to-end functionality of ASR by simulating a hardware fault. (See "Enable ILOM Telemetry" on page 4-4 for information on sending test alerts.) The end result is an email sent to the e-mail address of the My Oracle Support account associated with the ASR installation.

Note: The ASR Asset Menu (`asrassetmenu.sh`) is not available on ASR Assets running Solaris 11. To send a test email on an ASR Asset for Solaris 11, run the following command:

```
asradm send test email.address@mycompany.com
```

1. Execute the `asrassetbundle` shell script:

- If on an ASR Asset:

```
cd /untar_location_of_assetbundle/asrassetbundle
./asrassetmenu.sh
```

Note: If you have issues finding the `asrassetbundle` directory, go to "[Obtain the ASR Asset Bundle for non-ILOM Telemetry Sources](#)" on page 4-1 for more information.

- If on the ASR Manager system:

```
cd /opt/SUNWswasr/asrassetbundle
./asrassetmenu.sh
```

2. From the ASR Asset Menu, type **8**.
3. Whether you are on an ASR Asset or the ASR Manager, enter the IP address of the ASR Manager.
4. Enter the SNMP port used to send hardware telemetry to the ASR Manager. The default port is **162**.
5. When the test alert is sent, check the email account of the Sun Online Account associated with the ASR installation.

Note: If this test fails on Solaris 10, be sure that the `/usr/sfw/bin/snmptrap` exists and Solaris `net-snmp` library is installed on the asset.

5.1.4 Enable/Disable ASR Assets

Follow the procedures below to enable or disable ASR Asset(s). Regardless of which asset you wish to enable or disable, this action is always performed on the ASR Manager system. The most common reasons to disable ASR Asset(s) are for system maintenance or if an asset is “noisy” in terms of sending an excess of telemetry data. Disabling an ASR Asset stops the ASR Manager from sending fault telemetry to Oracle for that asset.

5.1.4.1 Disable ASR Assets

1. Open a terminal window and log in to the ASR Manager system as root.
2. Run any one of the following commands depending on your circumstance. Use the IP address or the hostname of the asset you wish to disable. If you disable the ASR Manager itself, only its telemetry will be stopped. **All enabled ASR Asset(s) that send telemetry to this ASR Manager will continue**, and the ASR Manager will continue to forward fault telemetry to Oracle’s backend systems.
 - `asr disable_asset -i IP_address`

- `asr disable_asset -h hostname`
- `asr disable_asset -s subnet`
(used to disable a group of assets within the subnet)

5.1.4.2 Enable ASR Assets

After you have disabled an ASR asset, you can re-enable it when you are ready for ASR to begin transmitting telemetry data.

1. Open a terminal window and log in to the ASR Manager system as root.
2. Run any one of the following commands depending on your circumstance. Use the IP address or the hostname of the asset you wish to enable. Once enabled, the asset will send hardware telemetry data to the ASR Manager and faults will be sent to Oracle's backend systems.
 - `asr enable_asset -i IP_address`
 - `asr enable_asset -h hostname`
 - `asr enable_asset -s subnet`
(used to enable a group of assets within the subnet)
3. Once complete, a successfully enabled message is displayed.
4. To confirm the asset is enabled, you can generate a test event using either one of the following command options:
 - `asr send_test -i IP_address`
 - `asr send_test -h hostname`

Note: The `asr send_test` command validates the ASR Manager connection to Oracle and the ASR activation status of the asset.

It does not validate the network connection from the asset to the ASR Manager.

5. The status of the test event is sent to the email address of the Sun Online Account associated with the ASR installation.

5.1.5 Deactivate/Activate ASR Assets

Deactivating an ASR Asset is done when you are replacing the asset or removing it entirely from the ASR system. When you deactivate an ASR Asset, ASR can no longer transmit telemetry data from this asset to Oracle.

Note: If you need to unregister your ASR Asset for Solaris 11, run:

```
asradm unregister
```

This command unregisters and disables your ASR Asset.

5.1.5.1 Deactivate/Activate ASR Assets from My Oracle Support

You can deactivate/activate ASR Assets from My Oracle Support. For more information see "[Review Assets in My Oracle Support](#)" on page 2-2.

1. In the "Assets" dashboard, click on the serial number of the asset you wish to deactivate/activate. The last column (ASR Status) will show the status of the asset (Active, Inactive, or Pending)

Serial Number	Asset Name	Product Name	Host Name	Support Identif...	Contact Name	ASR Status
0948	Cores2	S7410 Family	cores2-ar1	171	Carl	Active
07	Wayne Seltzer ...	SFV215,1x1.5,1...		171	Wayne Seltzer	Active
06		X4100 M2:2x222...		171	Jason	Active
060		X4100:2x252 4x1...	ASR-Asset2	171	Angelo	Active
071	Wayne Seltzer	SFV215,1x1.5,1...	unknown	171	Wayne Seltzer	Active - No Heartbeat
072		SE T5220 BASE ...		171		Pending
072		SE T5120 BASE ...		171		Pending
084		X4240:1x2347HE...		171		Pending
092		X2270:1xE5540,...		171		Pending
228		SFV880 4@900 ...		171		Pending
332		280R/2x1.2GHz/...		171		Pending
BEL		SE T5120 8CR 1...		171		Pending
BEL		FJ T5120 4CR 1....	unknown	171		Pending
FMS		SFV210,1x1GHz,...		171		Pending

2. In the Asset's Details pane, click the "Deactivate" button to deactivate the asset. If the asset is already deactivated, click the "Activate" button to activate it.
3. If necessary, you can update details about the asset (for example, change the Contact Name).

5.1.5.2 Deactivate/Activate ASR Assets from the ASR Manager

Follow these instructions to deactivate/activate an ASR Asset from the ASR Manager:

1. Open a terminal window and log in to the ASR Manager system as root.
2. Run any one of the following commands depending on your circumstance. Use the IP address or the hostname of the asset you wish to deactivate.
 - `asr deactivate_asset -i IP_address`
 - `asr deactivate_asset -h hostname`
 - `asr deactivate_asset -s subnet`
(used to enable a group of assets within the subnet)

Note: When you deactivate an ASR Asset, you cannot re-enable it. If you want to enable it again for ASR, you must re-activate it. Refer to ["Activate ASR Assets"](#) on page 4-7.

3. Once an asset is deactivated, you should also stop the hardware telemetry from being sent from the asset (even though the telemetry data is ignored by ASR once sent).

5.1.6 Add/Remove Telemetry Traps from ASR Asset(s)

The procedures in this section explain how to enable or disable telemetry trap destinations on ASR Asset(s). A trap destination is where the telemetry data is sent. During ASR installation, each asset is configured by setting trap destinations from the asset system. In all cases, the trap destination specified is the ASR Manager system,

which centrally collects the telemetry data sent from ASR Asset(s). Even if the ASR Manager itself is configured to send telemetry data, its trap destination must be this same ASR Manager.

Reasons for enabling traps include:

- Traps were not enabled during installation.
- Traps need to be enabled as part of troubleshooting tasks.

Reasons for disabling traps include:

- IP address of ASR Manager changed. If this situation occurs, you need to disable the traps, then re-enable the traps with the new IP information.
- Stopping the use of ASR and/or you want to minimize telemetry traffic.

Before continuing, be mindful of the following:

- You should know what telemetry sources exist on any particular ASR system. Refer to "[Confirm Existing Telemetry Sources](#)" on page 1-10.
- An active ASR Manager should already be fully installed. Refer to "[Install the ASR Manager](#)" on page 3-1.
- Ideally, but not required, at least one ASR Asset should already be fully installed. Refer to "[Configure and Manage ASR Assets](#)" on page 4-1.

5.1.6.1 Add/Remove Telemetry Traps from Solaris 10 FMA Systems

Follow the procedure below to add or remove a trap destination for systems using Solaris 10 FMA telemetry.

1. To add a Solaris FMA telemetry trap, go to "[Enable FMA Telemetry for Solaris 10 ASR Assets](#)" on page 4-2.
2. To remove a trap destination, make sure you are logged in as root on the system whose telemetry trap you wish to remove. This could be either an ASR Manager or an ASR Asset system. Keep in mind that this process stops telemetry from being sent to the ASR Manager. It does not remove the telemetry software itself nor disables its operation (for example, FMA).
3. Go to the directory where you previously untarred the ASR Asset Bundle file, and then go to the specific ASR Asset Bundle directory, if needed. For example:

- If on an ASR Asset:

```
cd /file_copy_location/asrassetbundle
```

- If on the ASR Manager system:

```
cd /opt/SUNWswasr/asrassetbundle
```

Note: Refer to "[Obtain the ASR Asset Bundle for non-ILOM Telemetry Sources](#)" on page 4-1 if you have issues locating the `asrassetbundle` directory and/or `asrassetmenu.sh` script (below).

4. Launch the ASR Asset Menu:

Note: If your ASR Asset system is running Solaris 11, you will use the `asradm` command. For all command options, run:

```
man asradm
```

```
./asrassetmenu.sh
```

```
Welcome to the ASR asset menu
```

```
-----
1) Check system for ASR qualifications
2) Add a trap-destination to SunMC agent
3) Add a trap-destination to FMA agent
4) Remove a trap-destination from SunMC agent
5) Remove a trap-destination from FMA agent
6) List SunMC agent trap-destinations
7) List FMA agent trap-destinations
8) Test event to verify ASR connectivity
9) Exit
```

5. Select 5 to remove the FMA trap destination.
6. When prompted, “. . . enter the number of the trap-destination to remove,” enter the list number of the IP address of the ASR Manager.

Note: If you are removing an FMA trap, enter the listed IP address with the port number (for example, 192.20.77.192:162).

7. The trap is then removed from the system and all telemetry sent from Solaris FMA to the ASR Manager is stopped.

5.1.6.2 Add/Remove Telemetry from Solaris 11 FMA Systems

Follow the procedure below to add or remove a trap destination for systems using Solaris 11 FMA telemetry.

1. To add a Solaris FMA telemetry trap, see ["Enable FMA Telemetry for Solaris 11 ASR Assets"](#) on page 4-4.
2. To delete the ASR Manager registration, run:

```
asradm unregister
```

5.1.6.3 Add/Remove Telemetry Traps from ILOM Systems

To add or remove an ILOM trap, refer to ["Enable ILOM Telemetry"](#) on page 4-4. This referenced procedure can be used to add or remove traps. If removing a trap, use the following parameters:

- If using the ILOM GUI interface, either remove the entire alert rule destination or set the **Level** parameter to **Disable**.
- If using the command line interface, set the **Level** parameter to **Disable**. Also, be sure to specify the correct alert rule (1 to 15) to disable.

5.1.6.4 Add/Remove Telemetry Traps from M-Series Systems (XSCF)

To add or remove telemetry traps on systems that have XSCF telemetry (Sun M-Series), refer to ["Enable M-Series XSCF Telemetry"](#) on page 4-6. This referenced procedure can be used to add or remove traps.

5.2 ASR Environment Management

This section provides a variety of procedures that can be used to manage the ASR environment as a whole.

5.2.1 Unregister ASR

When you installed ASR, you registered it with the transport server (transport.oracle.com) using your My Oracle Support username. The registration is performed on the ASR Manager system, as is an unregister if required. Reasons for unregistering ASR can include the following:

- If your current My Oracle Support account is no longer valid, as in a case when the email contact is no longer associated with the company. The email address associated with the My Oracle Support login is used by ASR to send a variety of ASR notifications, such as status reports. In this case, ASR should be unregistered and then re-registered with the new account information.
- If the server and ASR handshake becomes corrupted.

To unregister ASR:

1. From the ASR Manager system, run:

```
/opt/SUNWswasr/bin/asr unregister
```

2. Once unregistered, ASR cannot send hardware fault telemetry to Oracle's backend systems.

To register ASR, refer to "[Register the ASR Manager](#)" on page 3-6 for instructions.

5.2.2 Starting and Stopping ASR and OASM

This section explains how to stop and start your complete ASR environment. There are several reasons why you may want to do this, as listed below:

- Telemetry rules or other image upgrade to ASR.
- If you change network and port settings used by ASR. These changes are typically made in the OASM `config.ini` file:

```
/var/opt/SUNWsasm/configuration/config.ini
```

Note: On Solaris, OASM startup/restart is done via SMF service.

5.2.2.1 Stopping ASR and OASM

Follow the procedure below to stop ASR and OASM.

Note: Stopping OASM is optional, depending upon what your purpose is. If changes are made to the OASM `config.ini` file, for example, you must stop and restart OASM. In conformance with best practices, OASM should be stopped whenever ASR is stopped, and started whenever ASR is started.

1. Open a terminal window and log in as root on the ASR Manager system.
2. Run the following commands:
 - For Solaris:

```
/opt/SUNWasr/bin/asr stop-instance (stops ASR)
svcadm disable sasm (stops OASM)
```

- For Oracle Linux:

```
/opt/SUNWasr/bin/asr stop-instance (stops ASR)
/opt/SUNWsasm/bin/sasm stop-instance (stops OASM)
```

3. Once ASR is stopped, you can perform the desired maintenance tasks. Once complete, continue to the next section to restart ASR.

5.2.2.2 Starting ASR and OASM

Follow the procedure below to restart ASR and OASM:

1. Open a terminal window and log in as root on the ASR Manager system.

2. Run the following commands:

- For Solaris:

```
svcadm enable sasm (starts OASM)
/opt/SUNWasr/bin/asr start-instance (starts ASR)
```

- For Oracle Linux:

```
/opt/SUNWsasm/bin/sasm start-instance (starts OASM)
/opt/SUNWasr/bin/asr start-instance (starts ASR)
```

3. Be sure that ASR can send information to the transport.oracle.com servers by running the following command:

```
asr test_connection
```

5.3 ASR Emails

This section describes the types of emails generated by ASR. See "[ASR E-mail Examples](#)" for examples. Email generated by ASR is sent to:

- The email address of the My Oracle Support account associated with the ASR installation.
- The contact assigned to the asset in My Oracle Support.
- A distribution list assigned to the asset in My Oracle Support (optional)

The types of email generated by ASR include:

- **ASR Activation Email and Status of ASR Assets**

An email indicating success or failure of ASR activation is sent. Instructions for any user action is included as needed. ASR Asset status is available in My Oracle Support.

- **ASR Service Request Email**

Service Request emails are generated whenever a Service Request is created at Oracle that results from a hardware fault detection on any of your ASR-enabled systems. Failure emails indicate what issues may have prevented a Service Request from being created upon receipt of a hardware fault from ASR.

All Service Request emails are sent to the Primary and Preferred Technical Contact associated with the system reporting a potential fault. For more on how this contact is established or changed, refer to "[Review Assets in My Oracle Support](#)" on page 2-2.

Note: email sent from Blade ASR Assets have a different email format.

- **Heartbeat Failure Notification**

If the ASR Heartbeat detects a communications error to Oracle, an email is sent. The ASR Heartbeat should have been setup in a cron job during ASR installation, as discussed in "[Set Up Crontab](#)" on page 3-9.

- **Fault Rules Out of Date Email**

This email is sent if ASR detects that its fault rules are out of date. See "[Set Up Crontab](#)" on page 3-9 for more information on fault rules.

Note: If the `asr heartbeat` is disabled in crontab, you will not be notified, via email, if your ASR fault rules are out of date with the most current release. To be sure your fault rules are current, you can run the `asr update_rules` command from the ASR Manager system.

5.4 ASR Backup and Restore

ASR Backup

1. Verify all information is in the database that is activated. Run:
`/opt/SUNWswasr/bin/asr list_asset`
2. Stop OASM so that data does not change in middle of backup:
 - For Solaris, run: `svcadm disable sasm`
 - For Oracle Linux, run: `/opt/SUNWsasm/bin/sasm stop-instance`
3. Back up the database directory. Run:
`tar -cjf db.tar.bz /var/opt/SUNWsasm/db`
4. Create a backup of the ASR configuration. Run:
`tar -cjf configuration.tar.bz /var/opt/SUNWsasm/configuration`
5. Copy both `db.tar.bz` and `configuration.tar.bz` files to their proper backup destination.
6. Restart OASM. Run:
 - For Solaris, run: `/opt/SUNWsasm/bin/svcadm enable sasm`
 - For Oracle Linux, run: `/opt/SUNWsasm/bin/sasm start-instance`

ASR Restore

1. Install the ASR plugin and OASM:
 - For Solaris, run:
`pkgadd -d SUNWsasm.version_num.pkg`
`pkgadd -d SUNWswasr.version_num.pkg`
 - For Oracle Linux, run:
`rpm -i SUNWsasm.version_num.rpm`


```
rpm -i SUNWswasr.version_num.rpm
```

Note: Download and install the latest packages to upgrade to the latest version of the ASR Manager. See "[Download the OASM and ASR Packages](#)" on page 3-5 for more information.

2. Stop OASM to restore files:
 - For Solaris, run: `svcadm disable sasm`
 - For Oracle Linux, run: `/opt/SUNWasm/bin/sasm stop-instance`
3. Restore the files from backup:
 - a. Remove files `/var/opt/SUNWasm/configuration` and `/var/opt/SUNWasm/db`
 - b. Copy backup data to `/var/opt/SUNWasm/`
 - c. Extract the tar files (both Solaris and Oracle Linux):


```
tar -xvf configuration.tar.bz
tar -xvf db.tar.bz
```
4. Verify the files have been correctly extracted. Run:


```
ls /var/opt/SUNWasm/
```
5. Restart OASM. Run:
 - For Solaris, run: `svcadm enable sasm`
 - For Oracle Linux, run: `/opt/SUNWasm/bin/sasm start-instance`
6. Register the backup configuration. Run:


```
/opt/SUNWswasr/bin/asr register
```

Note: If you are running the latest version of ASR and if host name of the restored ASR Manager and My Oracle Support account) login have not changed, then you can stop here. Steps 7 and 8 are not required.

7. Remove old entries from the My Oracle Support backend to associate correctly. Run:


```
/opt/SUNWswasr/bin/asr send_deactivations -a
```
8. Add new entries to the My Oracle Support backend. Run:


```
/opt/SUNWswasr/bin/asr send_activations -a
```
9. List ASR Assets. Run:


```
asr list_asset
```

5.5 ASR Network Parameters Management

This section provides the instructions for networking-related tasks for ASR operations.

5.5.1 ASR Port Usage

The following table explains the network ports used by ASR:

Source	Destination	Protocol	Port	Description
ASR Asset	ASR Manager	http/https	<i>user defined</i>	For sending Solaris 11 ASR telemetry to the ASR Manager.
ASR Manager	ASR Backend (Oracle)	https	443	For sending telemetry messages to the ASR backend systems at Oracle.
ASR Manager	ASR Asset	http	6481	Service Tags listener for Asset activation
ASR Asset	ASR Manager	snmp udp	162	For sending telemetry messages to the ASR Manager.
ASR Manager	ASR Asset	snmp (get) udp	161	FMA enrichment for getting additional diagnostics information (Solaris 10 only).

5.5.2 Changing the Default SNMP Port for ASR

You can change the default SNMP port on the ASR Manager by editing the `/var/opt/SUNWsasm/configuration/config.ini` file as follows:

1. Change `com.sun.svc.container.snmp.port=162` to listen on whatever port is appropriate. **162** is the default.

2. Restart OASM:

```
svcadm restart sasm
```

3. Verify the change:

```
/opt/SUNWsasm/bin/sasm getprop | grep com.sun.svc.container.snmp.port
```

This command will return the new port value that you entered.

5.5.3 Configure ASR to Send HTTPS Traffic Through a Proxy Server

This procedure should be used to enable network communications in cases where you have a SOCKS proxy server mediating network traffic between the ASR Manager and the internet. For other proxy server types, you need to re-register ASR to set-up the proxy server information, as discussed in "[Register the ASR Manager](#)" on page 3-6.

1. Open a terminal window and log in as root to the ASR Manager system.
2. Using an editor of your choice (such as vi), edit the following file by changing the SOCKS proxy information as needed:

```
/var/opt/SUNWsasm/configuration/config.ini
```

3. The following entries must be made within the file. Contact a Network Administrator if needed.

```
socksProxyHost=  
socksProxyPort=  
java.net.socks.username=  
java.net.socks.password=
```

4. Restart ASR using the following command:

- For Solaris: `svcadm restart sasm`

- For Oracle Linux, run:

```
/opt/SUNWsasm/bin/sasm stop-instance
/opt/SUNWsasm/bin/sasm start-instance
```

5. To verify the changes, run the following command:

```
cat /var/opt/SUNWsasm/configuration/config.ini | grep socks
```

5.5.4 Configure OASM Network Settings

The following command can be used to confirm that the network parameters used by OASM to connect to Oracle's ASR backend systems are properly set:

```
grep transport.root
/var/opt/SUNWsasm/configuration/config.ini
```

The ASR transport hostname is displayed and will be similar to the results shown below:

```
com.sun.svc.container.transport.root=
https://transport.oracle.com
```

5.5.5 Test Connectivity from the ASR Manager to Oracle

The following procedure can be used to confirm proper communication between the ASR Manager and Oracle's ASR backend systems.

1. Complete **one** of the following steps from the ASR Manager to verify connectivity to Oracle's ASR backend systems:

- `telnet transport.oracle.com 443`
- If you have a web browser, go to `https://transport.oracle.com`. The web page should indicate that the Data Transport Service is operating.
- If a web browser is unavailable, run the following commands from a terminal window:

```
wget https://transport.oracle.com
```

2. If the results of the above commands do not indicate the Data Transport Service is operating, you must resolve your network connection issue. Listed below are possible resolutions:
 - The issue could be a DNS problem, or you might need to add `transport.oracle.com/141.146.156.46` to the `/etc/hosts` file.
 - You may need to contact your network administrator for assistance. Refer to "[Oracle Auto Service Request Configuration Requirements](#)" on page 1-7 for the specific ASR network requirements.
 - If you use a proxy server, the issue could be that the proxy information has not yet been configured to ASR and OASM. This is done by registering ASR, as discussed in the following procedure.

5.6 ASR Integration with Enterprise Monitoring Systems

Other environments are set up to use different enterprise monitoring systems (e.g., IBM Tivoli, HP OpenView, etc.). Beginning with ASR 3.0, integration with My Oracle Support allows sending ASR service-request information to these systems. Once

installed and properly configured, ASR provides the following integration features with enterprise monitoring systems:

- Ability to configure SNMP trap destination from OASM ASR to enterprise monitoring systems.
- Send case creation and test alert messages to enterprise monitoring systems.
- New ASR MIB that provides the data model of ASR case creation notification.

Examples of enterprise-monitoring systems include:

- IBM Tivoli
- HP OpenView
- BMC Patrol
- Unicenter
- xVM Ops Center
- Any monitoring tool that can receive an SNMP v2c trap

During installation of the ASR software package, the SNMP trap destination can be configured from the OASM host to monitoring systems. Once the ASR-capable assets are activated, ASR is designed to generate a service request after specific faults are detected. Once the service request is opened, the Oracle Support coverage and response times are delivered in accordance with your Oracle Premier Support or Warranty Contract.

Note: Because of ASR 3.0 integration with My Oracle Support, there are changes in the Service Request format. The service request number format in the notification trap is not correct if you are using any version older than ASR 3.0 manager. See "[Upgrade ASR](#)" on page 5-17 for instructions on upgrading to the latest version of ASR.

The OASM ASR Plugin polls the ASR backend whenever a fault event or test alert occurred and updates its local database with service request or test alert information. Once the service request/test alert information is available to the OASM ASR Plugin, it sends an SNMP v2c trap to the enterprise monitoring systems and include the following service request/test alert data defined in the ASR MIB:

- | | |
|--|---|
| ■ Hostname | ■ Link to Service Request number |
| ■ IP address | ■ Service Request status information (for "unable to create SR" problems) |
| ■ Serial number | ■ Severity of Service Request |
| ■ Platform type | ■ SR creation time |
| ■ Fault information (one line description) | ■ Fault detection time |
| ■ Fault information knowledge link | ■ Customer Contact information |
| ■ Service Request number | |

5.6.1 Configuring Trap Files

Follow the procedure below to configure trap files for ASR:

1. Set ASR notification trap destination:

```
/opt/SUNWswasr/bin/asr set_notification_trap -i <ip_address>  
-p <portNumber> -c <community string>
```

For example:

```
/opt/SUNWswasr/bin/asr set_notification_trap -i 127.0.0.1 -p 162 -c public
```

Note: Port “162” in the example is the destination port on your monitoring system. The notification trap will be sent **only** when a new service request (SR) is created successfully, and also when the test SR (test SNMP alert from the ASR asset menu) is successful

2. Show ASR notification trap destination:

```
asr show_notification_trap
```

3. Delete ASR notification trap destination:

```
asr delete_notification_trap
```

5.6.2 MIB Location and Data Elements

The SUN-ASR-NOTIFICATION-MIB file is located at:

```
/var/opt/SUNWsasm/configuration/SUN-ASR-NOTIFICATION-MIB.mib
```

Data Element	Description
sunAsrSrHostname	Hostname of the system for which the Service Request was created.
sunAsrSrIpAddress	IP address of the system for which the Service Request was created.
sunAsrSrSerialNumber	Product serial number of the system for which the Service Request was created. For chassis and blade systems, chassis serial number is used.
sunAsrSrPlatformType	Product Type of the system for which the Service Request was created.
sunAsrSrCreationDateTime	Date and time when the Service Request was created.
sunAsrSrFaultDetectionDateTime	Date and time when the fault was generated.
sunAsrSrCreationStatus	Status indicating the processing of Service Request creation.
sunAsrSrAdditionalInfo	Additional information associated with the fault can be added as name/value pairs. For example: <pre><additional-information name=chassis_host_name>chassisHostName</additional-information></pre> <pre><additional-information name=chassis_serial_number>chassisSerial</additional-information></pre>
sunAsrSrFaultSummary	Brief summary of the fault for which the Service Request was created.
sunAsrSrKnowledgeLink	Link to a knowledge article for the fault that was reported.
sunAsrSrNumber	Service request number

Data Element	Description
sunAsrSrLink	URL for accessing the Service Request information.
sunAsrSrSeverity	Severity of the Service Request opened for the reported fault.
sunAsrSrName	<ul style="list-style-type: none"> Customer contact information associated with the device reporting the fault. Name of Customer Contact associated with the Serial Number of the Device for which the Service Request was created.
sunAsrSrTelephone	Telephone number of Customer Contact associated with the Serial Number of the Device for which the Service Request was created.
sunAsrSrEmail	Email address of Customer Contact associated with the Serial Number of the Device for which the Service Request was created.

5.7 Uninstall ASR

The following procedure explains how to remove ASR completely, or partially for the purpose of an upgrade.

- Important:** If you wish to remove ASR for the long term, start with the procedures below. If you are removing ASR for a short time, or for an ASR upgrade, start at step 6.
- From all ASR Asset systems, remove telemetry traps that send hardware telemetry to the ASR Manager. Follow these steps:
 - Identify what telemetry sources reside on the systems. If uncertain, refer to ["Telemetry Sources: Overview and Check"](#) on page 1-10.
 - Remove the telemetry traps. Refer to [Add/Remove Telemetry Traps from ASR Asset\(s\)](#). If you are collecting telemetry from the ASR Manager itself, be sure to remove those traps as well.
- Deactivate all ASR Asset(s). Refer to [Deactivate/Activate ASR Assets](#).
- Deactivate the ASR Manager. Refer to [Deactivate/Activate ASR Assets](#).
- Unregister ASR. Refer to [Unregister ASR](#).

Important: If you are using other OASM plug-ins (for example SFT), the OASM transport service used by these plug-ins will be unregistered as part of this process. Consult your plug-in documentation to re-register the OASM transport service, if needed.

- Remove the ASR package from the ASR Manager system:
 - For Solaris: `pkgrm SUNWswasr`
 - For Oracle Linux: `rpm -e SUNWswasr`
- Remove the OASM package from the ASR Manager system. Removing this package is optional and is often done to reduce system overhead. If you have other applications running under OASM, do not remove it. Refer to ["Check for OASM Installation and Version"](#) on page 3-4 for more information on OASM.
 - For Solaris: `pkgrm SUNWasm`

- For Oracle Linux: `rpm -e SUNWsasm`
8. If you never intend to use ASR and OASM again, run the following command to remove leftover artifacts (OASM log files, ASR asset database, configuration files, etc.):

Warning: This command will remove all asset activation, configuration, and ASR log file data. Only remove these files if you want to **permanently** remove ASR from the system or node.

```
rm -r /var/opt/SUNWsasm
```

9. After completing the steps above, the uninstall of ASR is complete.

5.8 Upgrade ASR

Follow the steps below to upgrade ASR:

1. Uninstall ASR. Refer to "[Uninstall ASR](#)".
2. Obtain the new ASR and OASM packages. Refer to "[Download the OASM and ASR Packages](#)" on page 3-5.
3. Install the new OASM and ASR packages. If you did not remove OASM during the uninstall of ASR, you can still install the new OASM package.
 - Install OASM. Refer to "[Install the OASM Package](#)" on page 3-5.
 - Install ASR. Refer to "[Install the ASR Package](#)" on page 3-6. Be sure to register and activate the ASR Manager, as explained in the referenced instructions.

ASR General Troubleshooting

This section provides a variety of troubleshooting procedures for the ASR software.

Note: This section provides instructions for Solaris. When possible, corresponding Oracle Linux instructions are provided. Please see the appropriate Oracle Linux documentation for details for general administration commands.

6.1 ASR Diagnostic Utility

An ASR Diagnostic Utility is included to provide analysis support of any installation problems. This utility packages the data collected and stores it in a consistent, configurable location for later retrieval/delivery and analysis. The .zip file, which is created, will need to be sent to Oracle manually.

6.1.1 Utility Contents

The ASR Diagnostic Utility consists of the following files:

- `diag-config.properties` - property file for customizing the diagnostic utility configuration
- `asrDiagUtil.sh` - shell script for invoking the utility method
- `com.sun.svc.asr.util.diag.jar` - Java method for collecting diagnostic data
- `README` - a "readme" text file describing the utility

At command prompt, run `./asrDiagUtil.sh` and follow the on-screen instructions on where the diagnostic data file is being generated.

6.1.2 Delivery Model

The ASR Diagnostic Utility is available as part of the ASR software bundle. After you download the latest ASR software bundle, access and run the utility:

1. Install `SUNWswasr.<version>.<timestamp>.pkg` (see ["Install the ASR Package"](#) on page 3-6 for more information)
2. Verify the ASR Diagnostic Utility files are located under `/opt/SUNWswasr/util/diag`
3. Run the utility.

Note: Support for Oracle Linux begins with ASR 2.7.

6.1.3 Configure the ASR Diagnostic Utility

The `diag-config.properties` file consists a list of properties for specifying location of the configuration and log directories. It also contains "toggle switches" for enabling and disabling a particular data set to be collected:

- `com.sun.svc.asr.util.diag.home.directory` – The property for specifying where the diagnostic data .zip bundle will be generated. Default is current directory where the ASR Diagnostic Utility is located.
- `com.sun.svc.asr.util.diag.zip.file.prefix` – The property for configuring the diagnostic data .zip file's name.
- `com.sun.svc.asr.util.diag.zip.recursive` property – The property for enabling traversing into subdirectories of any configuration or log directories.

6.2 Service Tools Bundle (STB) Troubleshooting

This section provides a variety of steps to check on the state of the Service Tools Bundle (STB) that must installed on most ASR systems. If issues arise during the installation and operation of ASR, STB may be part of the issue.

6.2.1 Check the STB Agent

1. Open a browser window to the system you wish to check using the following command. Be sure to include the `/` (slash) after **agent**.

```
http://asr_system_hostname:6481/stv1/agent/
```

2. A response similar to the following will be displayed:

```
<st1:response>
<agent>
<agent_urn><agent urn number></agent_urn>
<agent_version>1.1.4</agent_version>
<registry_version>1.1.4</registry_version>
<system_info>
<system>SunOS</system>
<host><your host name></host>
<release>5.10</release>
<architecture>sparc</architecture>
<platform>SUNW,Sun-Fire-V215::Generic_137111-06</platform>
<manufacturer>Sun Microsystems, Inc.</manufacturer>
<cpu_manufacturer>Sun Microsystems, Inc.</cpu_manufacturer>
<serial_number>0707FL2015</serial_number>
<hostid><host ID number></hostid>
</system_info>
</agent>
</st1:response>
```

3. If you do not get a response from the Service Tags agent, consult the Service Tags man pages:

```
man in.stlisten
man stclient
```

6.2.2 Check the Service Tags Version

Follow the procedure below to check the Service Tags version:

1. Open a terminal window and log in as root to the ASR system you wish to check.
2. Run the following command to get the Service Tags version:

```
stclient -v
```

ASR requires Service Tags version 1.1.4 or later.

6.2.3 Check Service Tags Probe

Follow the procedure below to determine that the Service Tag discovery probe is running:

1. Open a terminal window and log in as root to the ASR system you wish to check.
2. To determine that the Service Tag discovery probe is running, run the following command:

```
svcs -l svc:/network/stdiscover
```

3. If the probe is running correctly, the following information is displayed:

```
fmri svc:/network/stdiscover:default
name Service Tag discovery probe
enabled true
state online
next_state none
state_time Wed Sep 03 21:07:28 2008
restarter svc:/network/inetd:default
```

6.2.4 Check Service Tags Listener

Follow the procedure below to determine that the Service Tags Listener is running:

1. Open a terminal window and log in as root to the ASR system you wish to check.
2. To determine if the Service Tags listener is running, run the following command:

```
svcs -l svc:/network/stlisten
```

3. If the listener is running correctly, the following information is displayed:

```
fmri svc:/network/stlisten:default
name Service Tag Discovery Listener
enabled true
state online
next_state none
state_time Wed Sep 03 21:07:28 2008
restarter svc:/network/inetd:default
xibreXR_US root@s4u-v215c-abc12
```

6.2.5 Unable to Contact Service Tags on Asset

This message indicates that the activation failed during Service Tags discovery. The issue can be either Service Tags is not installed on the ASR Asset or is installed but not running. Also the issue can be network connectivity between ASR Manager and the ASR Asset. Complete the following checks:

1. Check if Service Tags is installed and running on an ASR Asset. Run:

```
stclient -x
```

If you cannot run this command, either Service Tags is not installed or not online.

2. Check if the Service Tags services are installed and online using the following command:

```
svcs | grep reg
```

3. The results should be similar to the following example:

```
online Aug_23 svc:/application/stosreg:default
online Aug_23 svc:/application/sthwreg:default
```

4. If you cannot find these services, it means Service Tags is not installed on the ASR asset.

5. If the Service Tags services are online, check if `psncollector` is online. Run:

```
svcs | grep psncollector
```

6. The results should be similar to the following example:

```
online Sep_09 svc:/application/psncollector:default
```

7. Make sure that there are no TCP Wrappers installed on the ASR asset to prevent any service tags discovery issues. Run the following command from the ASR Manager system:

```
wget http://<assetHostNameOrIPAddress>:6481/stv1/agent/
```

8. If there are TCP wrappers installed on the ASR asset, edit `/etc/hosts.allow` on the asset by adding:

```
in.stlisten:<OASM host name>
```

6.2.6 Service Tags on Asset Reports Unknown or Empty Serial Number/Product Name

If serial number is empty or "unknown" complete the following steps:

1. Input the correct serial number using the SNEEP command:

```
/opt/SUNWsneep/bin/sneep -s <serial number>
```

Note: SNEEP is part of the Services Tools Bundle that is a prerequisite of ASR (for more information, see ["Install Service Tags"](#) on page 3-2)

2. For versions of SNEEP older than 2.6, enter the following command:

```
svcadm restart psncollector
```

Note: If you are using SNEEP version 2.6, it is not necessary to manually restart the `psncollector` after inputting the serial number.

3. You can view the serial number using the following URL:

```
http://<AgentipAddress>:6481/stv1/agent/
```

4. If product name is empty or "unknown" check if the Hardware Service Tags are installed and online. Run:

```
svcs | grep sthwreg
```

5. The results should be similar to the following example:

```
online Aug_23 svc:/application/sthwreg:default
```

6. If you cannot find this service, it means Hardware Service Tags are not installed on the ASR asset.

6.2.7 Activation Failed for Asset <asset name> Due to Data Error

This message indicates that the message creation failed because of bad or missing data. Most of the time, this error is the result of an incorrect or incomplete serial number or product name. To resolve this message, complete the following steps:

1. Verify the serial number using the SNEEP command:

```
sneep
```

2. If serial number is not correct then input the correct serial number using the following SNEEP command:

```
/opt/SUNWsneep/bin/setcsn -c <serial number>
```

Note: SNEEP is part of the Services Tools Bundle that is a prerequisite of ASR (for more information, see "[Install Service Tags](#)" on page 3-2)

3. For versions of SNEEP older than 2.6, run the following command:

```
svcadm restart psncollector
```

Note: If you are using SNEEP version 2.6, it is not necessary to manually restart the `psncollector` after inputting the serial number.

4. You can view the serial number using the following URL:

```
http://<AgentIPAddress>:6481/stv1/agent/
```

5. Check if the Hardware Service Tags are installed and online. Run:

```
svcs | grep sthwreg
```

6. The results should be similar to the following example:

```
online Aug_23 svc:/application/sthwreg:default
```

7. If you cannot find this service, it means Hardware Service Tags are not installed on the ASR asset.

6.2.8 Cannot Retrieve the OASM IP Address

This error message indicates that the ASR Asset activation failed because the Oracle Automated Service Manager (OASM) IP address could not be retrieved. The final step for activating an ASR Asset includes this command:

```
asr activate_asset -i <host IP address>
```

When activation fails, the following error message displays:

```
Cannot retrieve the SASM IP address, please add the SASM IP
address to /etc/hosts
```

You must edit the `/etc/hosts` file to update the localhost entry. For example, as root, change an entry that looks like this:

```
127.0.0.1    hostname123.com hostname123 localhost.localdomain localhost
```

to this:

```
127.0.0.1    localhost.localdomain localhost
```

6.2.9 Services are Disabled: `stdiscover` or `stlisten`

Service tag processes (`stlisten` and `stdiscover`) must be online in order to activate assets successfully.

1. Check to determine if the `stdiscover` or `stlisten` services are disabled. Run the following command:

```
svcs stlisten stdiscover
```

If the services have been disabled, the output would look like this:

STATE	STIME	FMRI
disabled	12:20:14	svc:/network/stdiscover:default
disabled	12:20:14	svc:/network/stlisten:default

2. To enable the `stdiscover` and `stlisten` services, run the following command:

```
svcadm enable stlisten stdiscover
```

3. Verify the services are online:

```
svcs stlisten stdiscover
```

Once the services have been enabled, the output would look like this:

STATE	STIME	FMRI
enabled	12:20:14	svc:/network/stdiscover:default
enabled	12:20:14	svc:/network/stlisten:default

6.3 Check the State of the SMA Service

The SMA service needs to be online in order to support Solaris FMA enrichment data properly. Prior to configuring FMA, complete the following steps:

1. To check that the state of the SMA service is online, run:

```
svcs sma
```

2. If SMA is online, the state should indicate online, as in the following example:

STATE	STIME	FMRI
online	15:40:31	svc:/application/management/sma:default

3. If SMA is not online, run the following command to enable it:

```
svcadm enable sma
```

4. Repeat these steps to confirm SMA is online.

6.4 Check the State of ASR Bundles

For diagnostic purposes, it may be necessary to check the state of various application bundles installed on the ASR Manager system using the following procedure.

1. Open a terminal window and log in as root to the ASR Manager.
2. Enter the following command:

```
asr diag
```

3. Review the results of this command below along with the settings you should see:

```
id State Bundle
263 ACTIVE com.sun.svc.asr.sw_1.0.0 /fragnebts=264, 265
264 RESOLVED com.sun.svc.asr.sw-frag_1.0.0 Master=263
265 RESOLVED com.sun.svc.asr.sw-rulesdefinitions_1.0.0 Master=263
266 ACTIVE com.sun.svc.ServiceActivation_1.0.0
```

The state of each bundle should be as follows:

- `com.sun.svc.asr.sw` bundle should be **ACTIVE**
 - `com.sun.svc.asr.sw-frag` should be **RESOLVED**
 - `com.sun.svc.asr.sw-rules definitions` should be **RESOLVED**
 - `com.sun.svc.ServiceActivation` should be **ACTIVE**
4. If any of these states are incorrect, enter the following commands:

```
asr stop
asr start
```

5. Repeat steps 1 to 3.
6. To ensure everything is working properly, run the following commands:

```
asr test_connection
asr send_test
```

6.5 ASR Log Files

When you are troubleshooting ASR, you can change the level of information displayed in the logs, and increase or decrease the number of logs that are saved before being overwritten. The logs are written to the `sw-asr.log` files. Log files are located on the ASR Manager system at `/var/opt/SUNWsasm/log`

There are four levels of logs:

1. **Fine:** Displays the highest level of information. It contains fine, informational, warnings and severe messages.
2. **Info:** Displays not only informational data, but also both warnings and severe messages. This is the default setting.
3. **Warning:** Displays warnings and severe messages.
4. **Severe:** Displays the least amount of information; severe messages only.

The default number of logs collected and saved is 5. Once that number is reached, ASR begins overwriting the oldest file. You have the option to change the number of logs collected and saved. If you are gathering as much information as possible in a short time, you might want to limit the number of logs saved to accommodate the larger files.

6.5.1 Set Log Level

Follow the procedure below to set logging levels:

1. Open a terminal window and log in as root on the ASR Manager system.
2. To view the current level of information being gathered, run:

```
asr get_loglevel
```

3. To change the logging level, run:

```
asr set_loglevel level
```

The choices for level are: **Fine**, **Info**, **Warning**, or **Severe**.

6.5.2 Set Log File Counts

Follow the procedure below to set log file counts:

1. Open a terminal window and log in as root on the ASR Manager system.
2. To view the current number of logs being saved, enter the following command:

```
asr get_logfilecount
```

3. To change the number of logs being saved, enter the following command:

```
asr set_logfilecount <number>
```

6.6 Installing ASR Manager on Blade Systems

Before installing ASR Manager on a blade system, make sure the service `svc:/milestone/multi-user-server` status is online.

- To check the status of this service, run:

```
svcs svc:/milestone/multi-user-server
```

- If the state indicates maintenance, run:

```
svcadm clear svc:/milestone/multi-user-server  
svcadm enable svc:/milestone/multi-user-server
```

- If the state indicates disabled, run:

```
svcadm enable svc:/milestone/multi-user-server
```

6.7 Installing ASR Manager on a Local Zone

If the ASR Manager is installed on a local zone, it is not possible to activate the ASR Manager as an ASR asset. If this is attempted, an error will be received: *Asset cannot be activated due to unknown product name or serial number*. This is a known issue expected to be corrected in a future version of ASR.

6.8 Miscellaneous Errors and Resolution

This section provides a variety of error conditions and resolution steps.

6.8.1 Error Messages and Resolutions

Error Message	Resolution
WARNING: Unable to retrieve fault details. For additional information and some insights into how to correct, please see the ASR Installation and Operations Guide - located at www.oracle.com/asr . See the ASR General Troubleshooting Section.	<ol style="list-style-type: none"> 1. Verify that the asset has got the right Solaris minimum required version and patch level as per the ASR qualified systems web page (see http://www.oracle.com/asr for more information). 2. Review the community string properties on the asset. ASR Manager requires public as the value of the community string in order to retrieve FMA enrichment and additional fault details. (See "Enable M-Series XSCF Telemetry" on page 4-6 for more details) 3. Review the FMA trap destination configuration file, and restart <code>sma</code> and <code>fmd</code> SMF services.
WARNING: This trap is rejected because the asset is disabled	<p>Enable the ASR Asset using one of the following commands:</p> <pre>asr enable_asset -i <ip></pre> <p>(where <i>ip</i> is the IP address of the ASR asset)</p> <p>or</p> <pre>asr enable_asset -h <host></pre> <p>(where <i>host</i> is the hostname of the ASR asset)</p>
WARNING: this trap is rejected because OASM ASR Plug-in is not activated	<p>Enable the ASR Manager using one of the following commands:</p> <pre>asr activate_asset -i <ip></pre> <p>(where <i>ip</i> is the IP address of the ASR asset)</p> <p>or</p> <pre>asr activate_asset -h <host></pre> <p>(where <i>host</i> is the hostname of the ASR asset)</p>
WARNING: this trap is rejected because the asset is not found	<p>Enable the ASR Asset using one of the following commands:</p> <pre>asr activate_asset -i <ip></pre> <p>(where <i>ip</i> is the IP address of the ASR asset)</p> <p>or</p> <pre>asr activate_asset -h <host></pre> <p>(where <i>host</i> is the hostname of the ASR asset)</p>
SEVERE: Cannot attach snmp trap to snmp service!	<p>This indicates that there could be another process using port 162. Kill that process and then run:</p> <pre>svcadm restart sasm</pre>
Failure to Register Errors	<p>The <code>sasm.log</code> has more detailed information and a Java stacktrace on what failed during registration. When a failure error is encountered, additional details can be found in:</p> <pre>/var/opt/SUNWsasm/configuration/sasm.log</pre>
No Such Host Exception	<p>This error indicates that the host running ASR Manager cannot resolve the IP address for the Data Transport Service server. Refer to Section 5.5.5, "Test Connectivity from the ASR Manager to Oracle" to troubleshoot and resolve the problem.</p>

Error Message	Resolution
Not Authorized. The Sun Online Account provided could not be verified by the transport server	This error indicates that the communication between transport server and Oracle is down or busy. This can also indicate that the queue set-up is wrong or that the user does not have permissions to the queue.
Socket Exception: Malformed reply from SOCKS server	This error indicates one of the following: <ul style="list-style-type: none"> ■ The socks configuration in the <code>config.ini</code> file is incorrect or missing. Action: This usually indicates that you need to supply a user/password for the socks settings. ■ The socks is not able to route to the transport server endpoint. Action: Add the correct http proxy information or socks settings. Refer to "Configure ASR to Send HTTPS Traffic Through a Proxy Server" on page 5-12 to correct the information.

6.8.2 Only One Client Can Access Console at a Time

If you get this error message running an ASR command on the ASR Manager system, it indicates that only one command can go into the OASM admin port at a time. Each command has a max handle on the connection for 60 seconds before OASM console kills the connection. Try executing the command after 60 seconds. If you still get same message, do the following:

1. Check if OASM is running:

```
ps -ef | grep SUNWsasm
```

Results:

```
root 16817 1 0 16:09:49 ? 4:24 java -cp
/var/opt/SUNWsasm/lib/com.sun.svc.container.ManagementTier.jar:/var/opt
```

2. If OASM is running, kill the process using the following command:

```
kill -9 <Process_ID>
```

3. Restart the OASM using the following command:

```
svcadm restart sasm
```

6.9 ASR Fault Rules Updates

ASR uses fault rules to filter the telemetry data sent from ASR Assets. This filtering is done to remove telemetry that contains no real fault data and general telemetry “noise.” The filtering process also ensures that telemetry that contains faults is reported. These fault rules can change as ASR improves its filtering and as new platforms and telemetry sources are supported by ASR.

ASR installs a cron job on the ASR Manager system to periodically check Oracle’s auto-update server for any new rules updates. When there are new rules, the ASR Manager automatically downloads and installs the latest rules bundle. If the cron job is not set to download the fault rules automatically, an e-mail is sent to:

- The e-mail address of the My Oracle Support account associated with the ASR installation.
- The contact assigned to the asset in My Oracle Support.
- A distribution list assigned to the asset in My Oracle Support (optional)

For more information on fault rules, refer to:

- ["Set Up Crontab"](#) on page 3-9
- ["ASR Emails"](#) on page 5-9

Note: If the `asr heartbeat` is disabled in crontab, you will not be notified, via e-mail, if your ASR fault rules are out of date with the most current release. To be sure your fault rules are current, you can run the `asr update_rules` command from the ASR Manager system.

6.10 ASR Manager Crashed, Move Assets to a New ASR Manager

In cases where an ASR Manager experiences a critical failure, you can set up a new ASR Manager and reconfigure ASR Assets to report to the new host. The following steps describe a sample scenario:

1. An ASR Manager is set up (e.g., hostname: **ASRHOST01**, IP address: **10.10.10.1**) and configured on the network. This ASR host is registered and activated to itself.
2. All ASR assets are configured to report failures to the ASR Manager host (**ASRHOST01**), and all ASR assets are activated on the host.
3. A critical failure occurs in the cabinet of **ASRHOST01** (for example: a fire destroys the system and its data). The assets need to be attached to a different ASR Manager host (e.g., hostname: **ASRHOST02**).
4. A new ASR Manager is set up (e.g., hostname: **ASRHOST02**, IP address: **10.10.10.2**) and configured on the network. The new ASR host is registered and activated to itself.
5. All ASR assets are now re-configured to report failures to the new ASR Manager host **ASRHOST02**, and the trap destination is changed to report failures to **ASRHOST02**.
6. All ASR assets are now activated on **ASRHOST02**

Note: In order to reduce the additional work with moving the ASR Manager to a different location (e.g., from **ASRHOST1** to **ASRHOST2**), you can create an ASR backup on another host or on the existing host. Creating a backup is crucial when recovering from a crash (see ["ASR Backup and Restore"](#) on page 5-10 for a details on creating an ASR backup).

6.11 ASR - No Heartbeat

The ASR Manager must be configured correctly to send the daily cron job for `asr heartbeat`. After 50 hours, the unit will be marked as a 'Heartbeat Failure' unit.

If an ASR Manager is in Heartbeat Failure mode for 90 days, it will be automatically deactivated at the ASR backend and in My Oracle Support. Also, any assets that are configured via that ASR Manager will also be marked deactivated. This will prevent any future events creating automatic Service Requests.

You can check to see if any ASR Manager or ASR Asset are in *Heartbeat Failure* by reviewing the ASR status in My Oracle Support.

If you feel that ASR Manager is configured correctly, then you can troubleshoot your ASR Manager hardware to resolve the problem. See MOS knowledge article 1346328.1 for the instructions to your particular hardware:

<https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&doctype=HOWTO&id=1346328.1>

See [Appendix A.3, "Heartbeat Failure Notification E-mail Examples"](#) for an e-mail example you may receive should this problem occur.

6.12 ASR Assets for Solaris 11

In cases where you are having issues with configuring ASR on Solaris 11 assets using the `asradm` command, then review the status of the following `asr-notify` SMF service:

```
svcs asr-notify
```

Output should look like this:

```
STATE      STIME      FMRI
online     13:00:31   svc:/system/fm/asr-notify:default
```

Note: If the `asr-notify` service status is in maintenance mode, then clear the maintenance mode:

```
svcadm clear asr-notify
```

re-register the Solaris 11 asset with ASR manager

ASR E-mail Examples

This appendix provides email examples of what you can expect to receive from ASR. E-mails could be sent to:

- The e-mail address of the My Oracle Support account associated with the ASR installation.
- The contact assigned to the asset in My Oracle Support.
- A distribution list assigned to the asset in My Oracle Support (optional)

A.1 ASR Activation E-mail Examples

A.1.1 Activation Pending My Oracle Support

From: no.reply@oracle.com
Subject: Oracle ASR: Action Required - Activation is Pending
To: undisclosed-recipients;;

Serial#: <serial number>

Oracle Auto Service Request (ASR) activation for this asset is Pending.

To complete the activation process please login to My Oracle Support. (Use the menus - More... Settings... Pending ASR Activations).

Assets with a Pending status require approval in My Oracle Support. Note, to approve an ASR Pending activation, your My Oracle Support account must have the administrator privilege for the Support Identifier associated with the asset.

The Oracle Auto Service Request documentation can be accessed on

<http://oracle.com/asr>.

Please use My Oracle Support <https://support.oracle.com> for assistance.

A.1.2 Activation Failed

From: no.reply@oracle.com
Subject: Oracle ASR: Activation Request has not been Successful
To: undisclosed-recipients;;

Serial#: <serial number> Reason: <Reason will be indicated>
Serial#: <serial number> Reason: <Reason will be indicated>

Once resolved, please attempt asset activation for the asset again.

The Oracle Auto Service Request documentation can be accessed on
<http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.1.3 Activation Status Change

From: no.reply@oracle.com
Subject: Oracle ASR: Asset Status Change
To: undisclosed-recipients;;

Your Auto Service Request (ASR) asset has changed activation status.

Serial#: <serial number> has changed activation status to: ASR has been De-Activated.
Serial#: <serial number> has changed activation status to: ASR has been De-Activated.
Serial#: <serial number> has changed activation status to: ASR has been De-Activated.

Please login to My Oracle Support to see the status of your Oracle Auto Service Request (ASR) assets. (Use the menus - More... Settings... Assets).

Assets with an Active status are enabled and Service Requests specific fault events for these assets will cause Service Requests to be created.

Assets with a Pending status require approval in My Oracle Support. Note, to approve an ASR Pending activation, your My Oracle Support account must have the administrator privilege for the Support Identifier associated with the asset.

The Oracle Auto Service Request documentation can be accessed on
<http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.1.4 Activation Bad Serial

From: no.reply@oracle.com
Subject: Oracle ASR: Warning - Unable to Activate Asset
To: undisclosed-recipients;;

Serial#: <serial number>

Oracle Auto Service Request (ASR) is not able to complete your activation request. Please confirm that this is the correct serial number for the asset. Once the issue with the serial number has been corrected, reactivate the asset.

The Oracle Auto Service Request documentation can be accessed on <http://oracle.com/asr>. Please use My Oracle Support <https://support.oracle.com> for assistance.

A.1.5 Activation Denied

From: no.reply@oracle.com
Subject: Oracle ASR: Warning - Unable to Process Activation Request
To: undisclosed-recipients;;

Serial#: <serial number>

Oracle Auto Service Request (ASR) was unable to process your activation request because this asset is already activated by a different ASR manager.

The Oracle Auto Service Request documentation can be accessed on <http://oracle.com/asr>. Please use My Oracle Support <https://support.oracle.com> for assistance.

A.1.6 Status Report

From: no.reply@oracle.com
Subject: Oracle ASR: Asset Status Report
To: undisclosed-recipients;;

Please login to My Oracle Support to see the status of your Oracle Auto Service Request(ASR) assets.

(Use the menus - More... Settings... Assets).

Assets with an Active status are enabled and Service Requests specific fault events for these assets will cause Service Requests to be created.

Assets with a Pending status require approval in My Oracle Support. Note, to approve an ASR Pending activation, your My Oracle Support account must have the administrator privilege for the Support Identified associated with the asset.

The Oracle Auto Service Request documentation can be accessed on <http://oracle.com/asr>. Please use My Oracle Support <https://support.oracle.com> for assistance.

A.2 ASR Service Request E-mail

A.2.1 Test Create Success Example

From: no.reply@oracle.com
Subject: Oracle ASR: *Test* Service Request
To: undisclosed-recipients;;

Service Request test-create was successful.

The Oracle Auto Service Request documentation can be accessed on

<http://oracle.com/asr>.

Please use My Oracle Support <https://support.oracle.com> for assistance.

A.2.2 Test Create Fail Example

From: no.reply@oracle.com
Subject: Oracle ASR: Warning - Test Service Request failed
To: undisclosed-recipients;;

Serial#: <serial number>

Oracle Auto Service Request (ASR) was unable to verify Service Request because:

STATUSCHANGE

The Oracle Auto Service Request documentation can be accessed on

<http://oracle.com/asr>.

Please use My Oracle Support <https://support.oracle.com> for assistance.

A.2.3 Service Request Create Success Example

From: no.reply@oracle.com
Subject: Oracle ASR: Service Request <Service Request Number> Created
To: undisclosed-recipients;;

Service Request: <service request number>

Oracle Auto Service Request (ASR) has created a Service Request (SR) for one of your Activated ASR assets.

Please login to My Oracle Support to see the details of this SR. My Oracle Support can also be used to make any changes to the SR or to provide additional information.

The Oracle Auto Service Request documentation can be accessed on

<http://oracle.com/asr>.

Please use My Oracle Support <https://support.oracle.com> for assistance.

A.2.4 Service Request Create Failed Example

From: no.reply@oracle.com
Subject: Oracle ASR: Warning - Unable to Create Service Request
To: undisclosed-recipients;;

Serial#: <serial number>

Oracle Auto Service Request (ASR) was unable to create Service Request because:
<Reason for failure>

The Oracle Auto Service Request documentation can be accessed on
<http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.2.5 Partner Service Request Create Example

From: no.reply@oracle.com
Subject: Oracle ASR: Service Request <Service Request Number> Created
To: undisclosed-recipients;;

Service Request: <service request number>

Oracle Service Delivery Partner,

One of your customer's systems has logged an Automatic Service Request with Oracle.
A draft Service Request has been created within My Oracle Support.
This draft will remain active for the next 30 days.

To view the draft Service Request:

1. Log in to My Oracle Support.
2. Click on "Service Requests" in the menu area.
3. In the "Draft Service Requests" section, click on Service Request <Service Request Number>.
4. In the "Select Product" section, review the Support Identifier and Product Name.
5. In the "Describe Problem" section, review the "Detailed Description" for the fault details.

If you determine that you need assistance from Oracle to resolve the problem, enter the required information in draft Service Request and submit.

The Oracle Auto Service Request documentation can be accessed on
<http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.2.6 Service Request Create is Delayed Example

From: no.reply@oracle.com
Subject: Oracle ASR: Warning - Service Request Creation is Delayed
To: undisclosed-recipients;;

Serial#: <serial number>

Oracle Auto Service Request (ASR) is attempting to create a Service Request (SR) for this asset; however, it is unable to at this time.

ASR will continue to attempt to create the Service Request.

You may use My Oracle Support <https://support.oracle.com> to manually create an SR for this asset.

The Oracle Auto Service Request documentation can be accessed on <http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.2.7 Draft Service Request Example (non-Partner)

From: no.reply@oracle.com
Subject: Oracle ASR: Draft Service Request <Service Request Number> Created
To: undisclosed-recipients;;

Service Request: <Service Request Number>

One of your systems has logged an Automatic Service Request with Oracle.

A draft Service Request has been created within My Oracle Support.

This draft will remain active for the next 30 days.

To view the draft Service Request:

1. Log in to My Oracle Support.
2. Click on "Service Requests" in the menu area.
3. In the "Draft Service Requests" section, click on Service Request <Service Request Number>.
4. In the "Select Product" section, review the Support Identifier and Product Name.
5. In the "Describe Problem" section, review the "Detailed Description" for the fault details.

If you determine that you need assistance from Oracle to resolve the problem, enter the required information in draft Service Request and submit.

The Oracle Auto Service Request documentation can be accessed on <http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.3 Heartbeat Failure Notification E-mail Examples

A.3.1 Heartbeat Failure - CAM

From: no.reply@oracle.com
Subject: Oracle ASR: Warning - Connectivity Failure
To: undisclosed-recipients;;

Serial#: <serial number>

Oracle Auto Service Request (ASR) has detected a Heartbeat Failure for this asset.
ASR would not be able to create a Service Request (SR) if a fault were to occur.
Please review the CAM documentation to resolve.

Once the network issues are resolved, all queued alerts will be transmitted and SR's opened as needed.

The Oracle Auto Service Request documentation can be accessed on
<http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.3.2 Heartbeat Failure - Sun Unified Storage 7xxx

From: no.reply@oracle.com
Subject: Oracle ASR: Warning - Connectivity Failure
To: undisclosed-recipients;;

Serial#: <serial number>

Oracle Auto Service Request (ASR) has detected a Heartbeat Failure for this asset.
ASR would not be able to create a Service Request (SR) if a fault were to occur.
Please review the Oracle Unified Storage documentation to resolve.

Once the network issues are resolved, all queued alerts will be transmitted and SR's opened as needed.

The Oracle Auto Service Request documentation can be accessed on
<http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.3.3 Heartbeat Failure - ASR SO

From: no.reply@oracle.com
Subject: Oracle ASR: Warning - Connectivity Failure
To: undisclosed-recipients;;

hostname: <hostname>

Oracle Auto Service Request (ASR) has detected a Heartbeat Failure for this asset.
ASR would not be able to create a Service Request (SR) if a fault were to occur.
The ASR service has not received any communication from the ASR Manager during the last 50 hours.

If a fault event on any of the ASR-enabled assets were to occur, ASR would be unable to create a Service Request.

Please review the documentation to resolve this problem.

To resolve this problem, please check:

- Is ASR Manager heartbeat enabled in cron?
'crontab -l | grep heartbeat' command shows the heartbeat cron entry.
- Is ASR Manager running?
'asr diag' command provides a short status listing of ASR Manager bundles.
- Is ASR Manager registered with Oracle?
'asr show_reg_status' command shows the registration status.
- Is ASR Manager able to communicate with Oracle?
'asr test_connection' command performs a transport test.

The Oracle Auto Service Request documentation can be accessed on <http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.

A.4 Fault Rules Out of Date E-mail

From: no.reply@oracle.com
Subject: Oracle ASR: Fault Rules are Out of Date
To: undisclosed-recipients;;

hostname: <hostname>

The Oracle Auto Service Request (ASR) fault rules are out of date on this ASR Manager.
The latest version is <version number>

On the ASR Manager please run the following command:

```
asr update_rules
```

This will download the latest fault rules version and update the ASR rules.

The Oracle Auto Service Request documentation can be accessed on <http://oracle.com/asr>.
Please use My Oracle Support <https://support.oracle.com> for assistance.